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

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

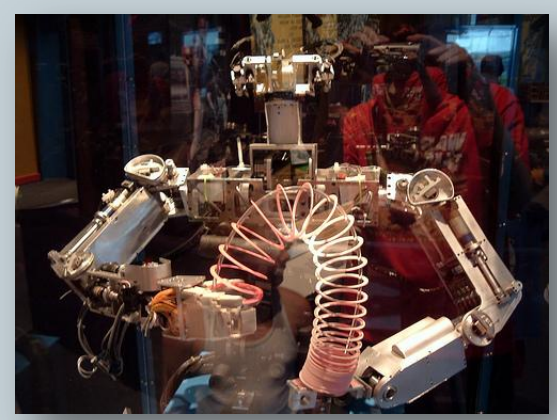
Computer Science and Engineering
University of Washington

Focus of This Talk: Robots, Security, and Privacy

- 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)



CC images courtesy of: http://www.flickr.com/photos/bbum/133956572/, http://www.flickr.com/photos/deadair/220147470/, http://www.flickr.com/photos/cmpalmer/3380364862/

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?

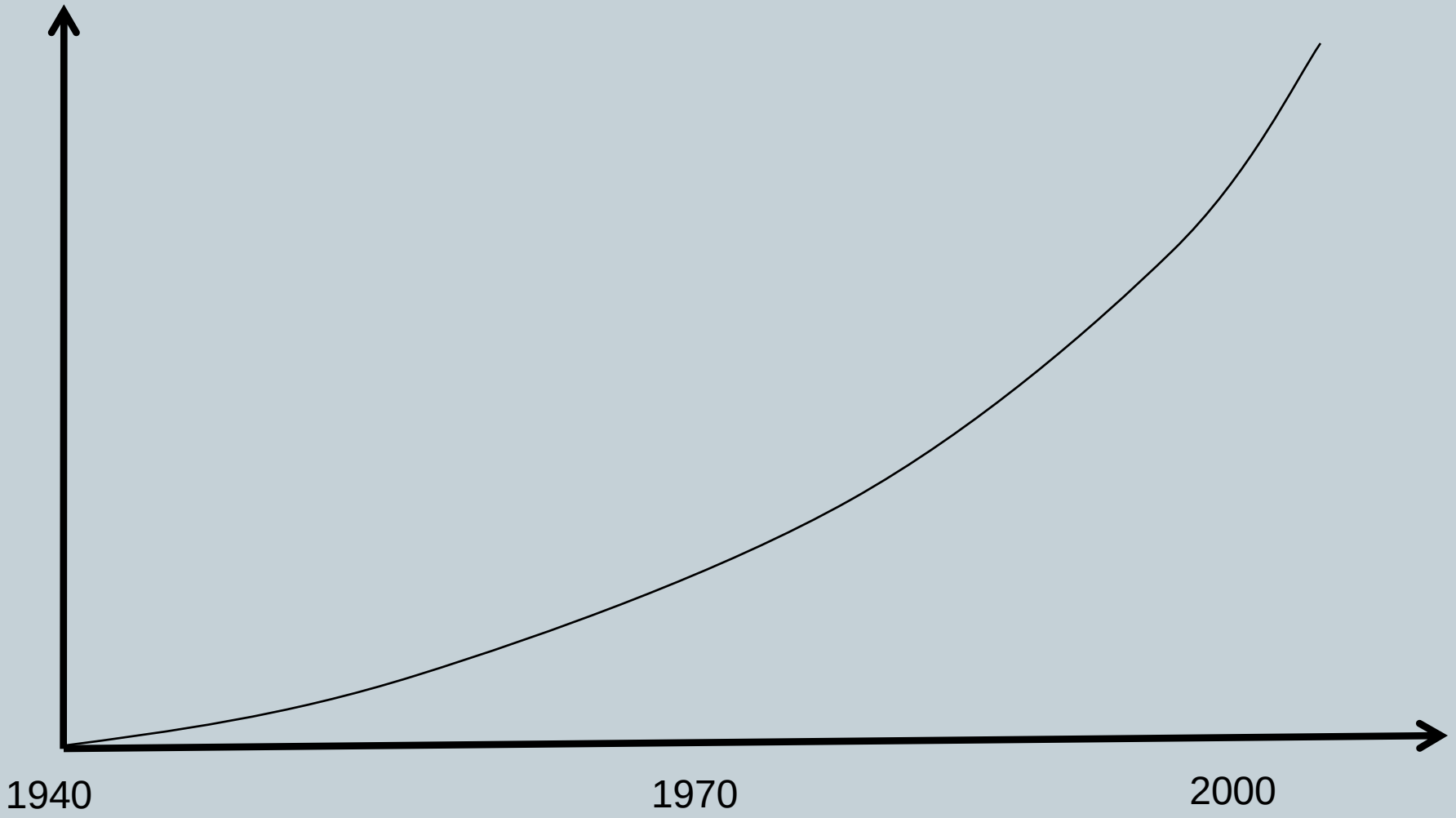
- Security:
  - Systems behave as intended even in the presence of an adversary
- NOT Safety:
  - Systems behave as intended even in the presence of accidental failures

Security for Robots?

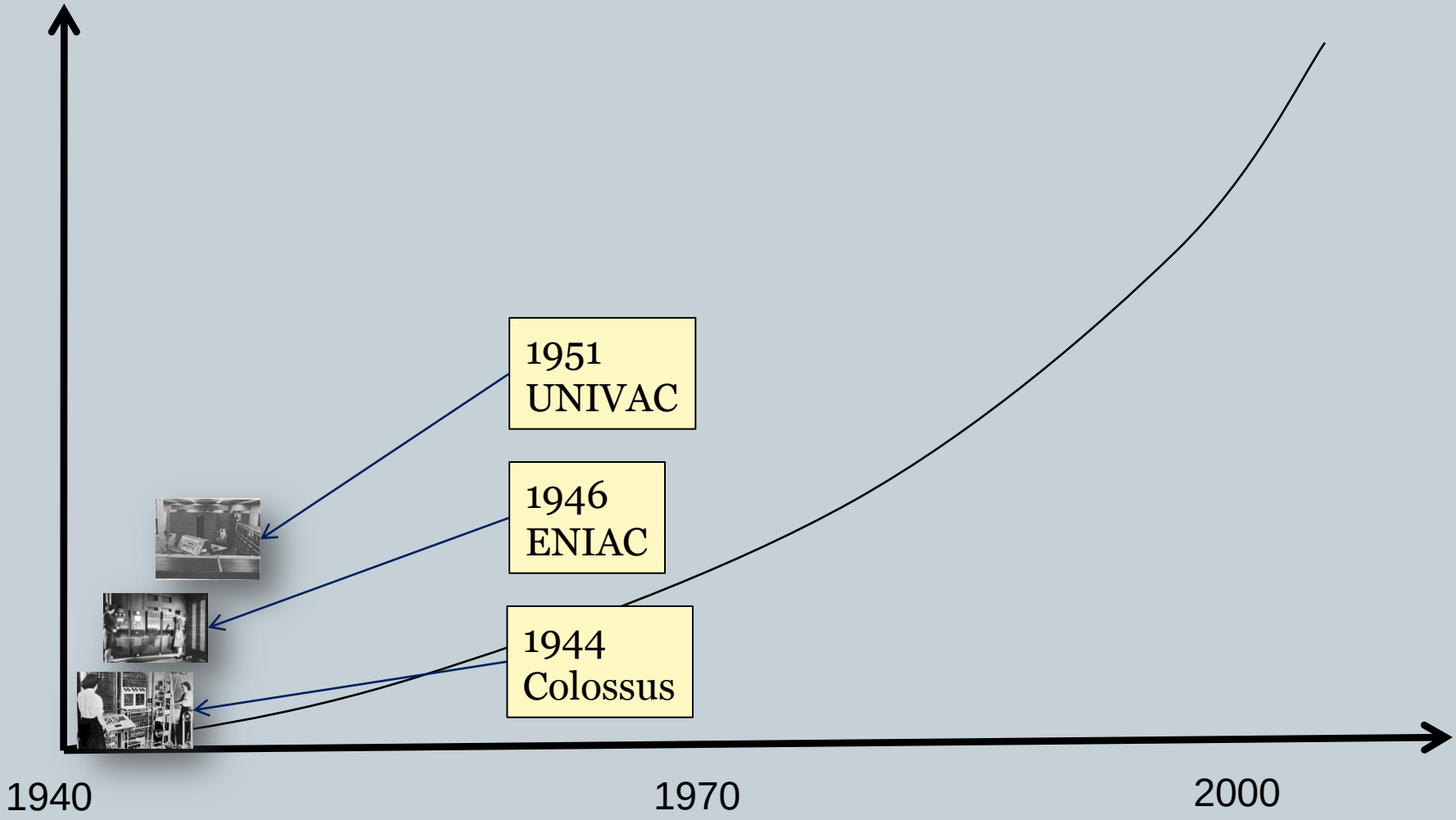
- To understand the importance of security for robots, we give context:

  A brief history of computers and computer security.

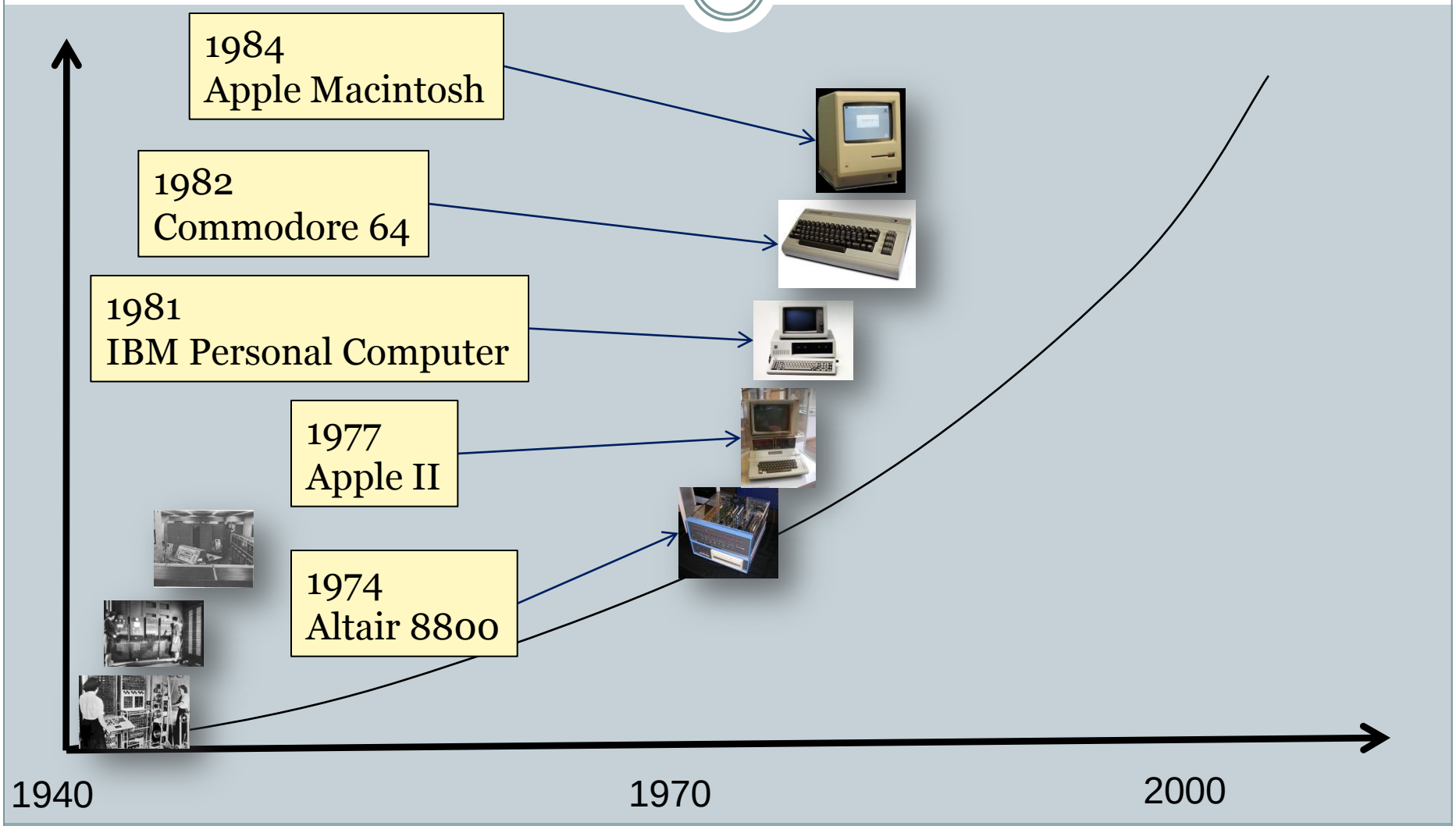
Timeline: Computers



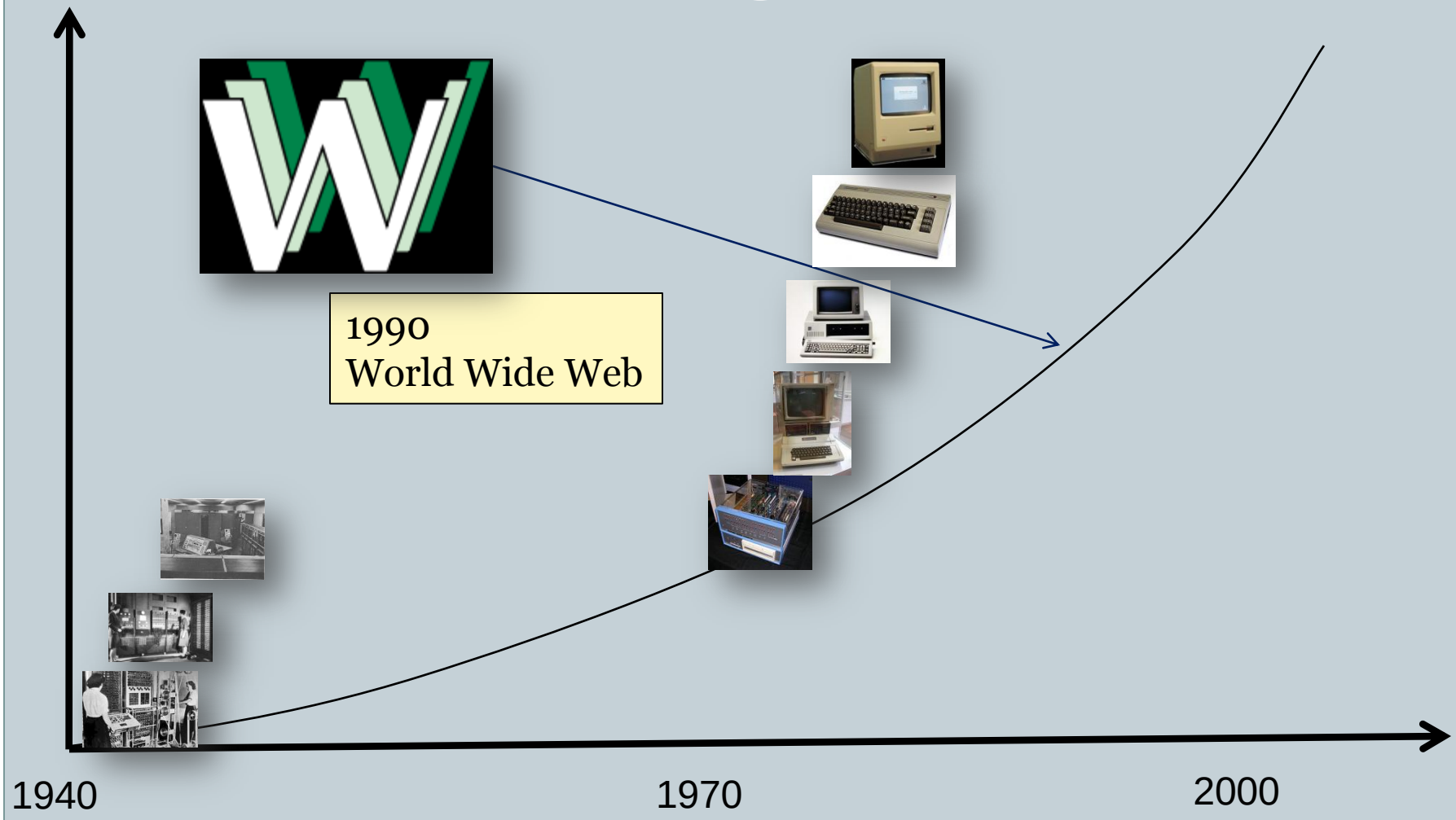
Timeline: Computers



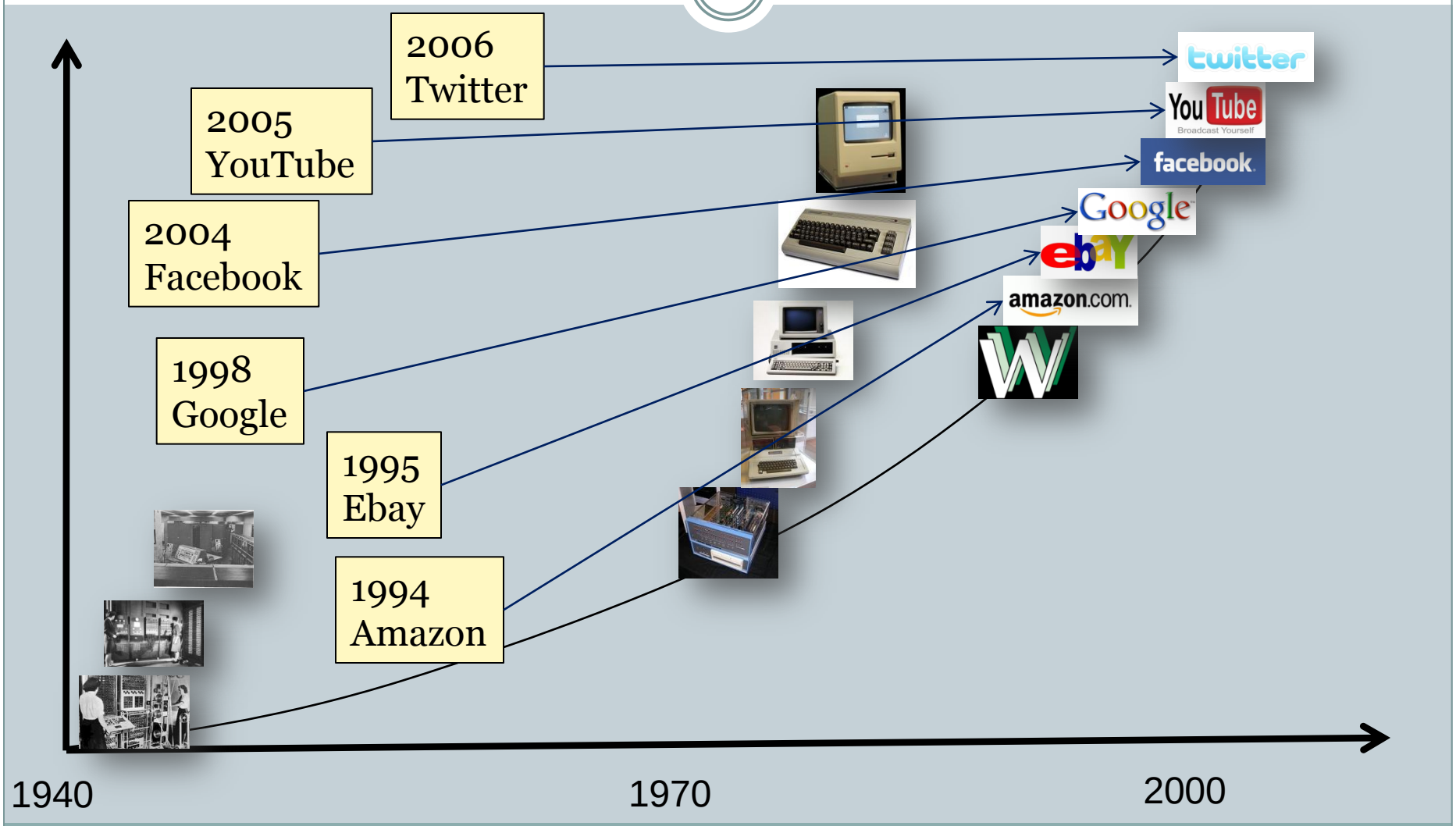
Timeline: Computers



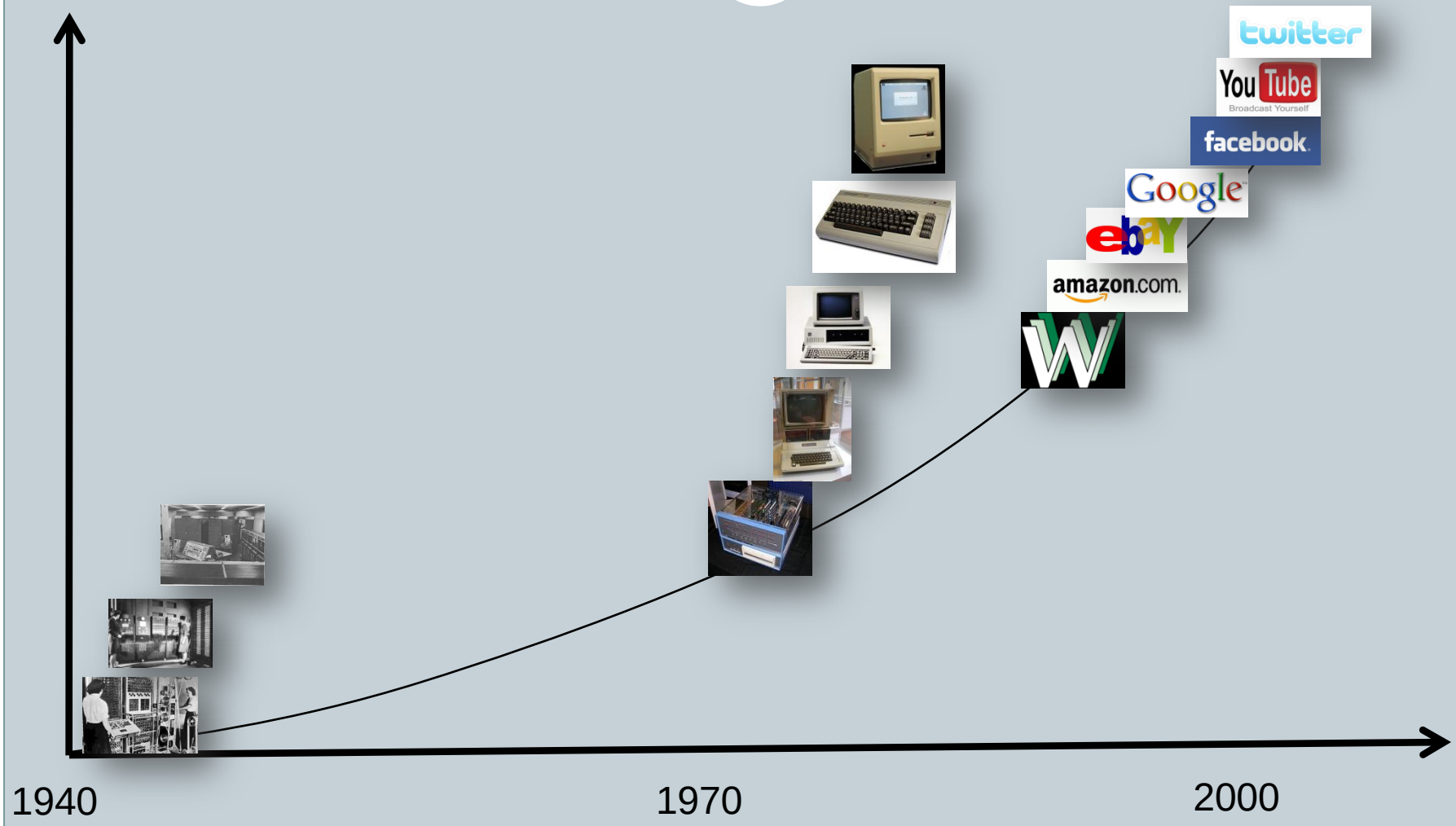
Timeline: Computers



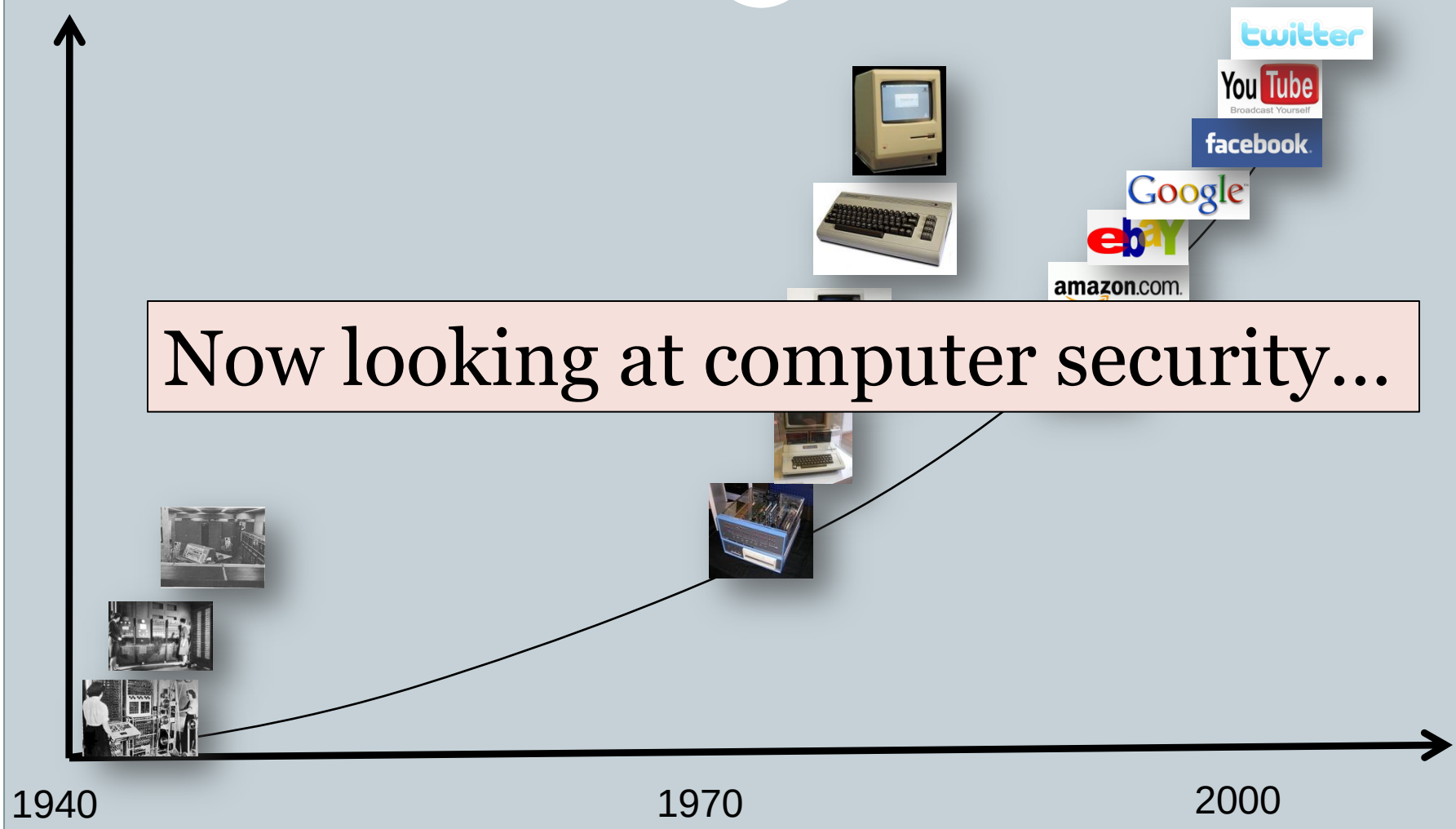
Timeline: Computers



Timeline: Computers

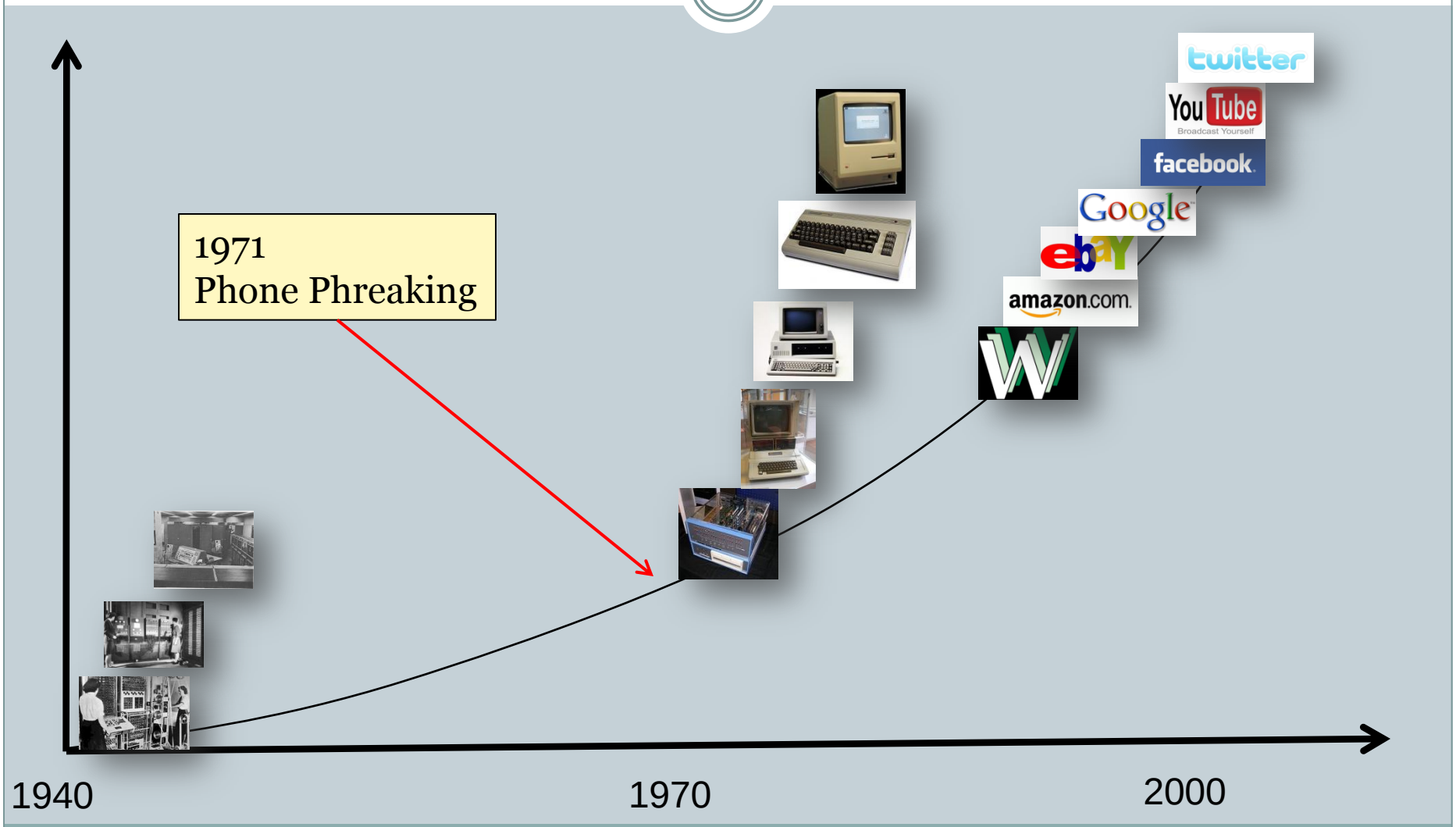


Timeline: Computers

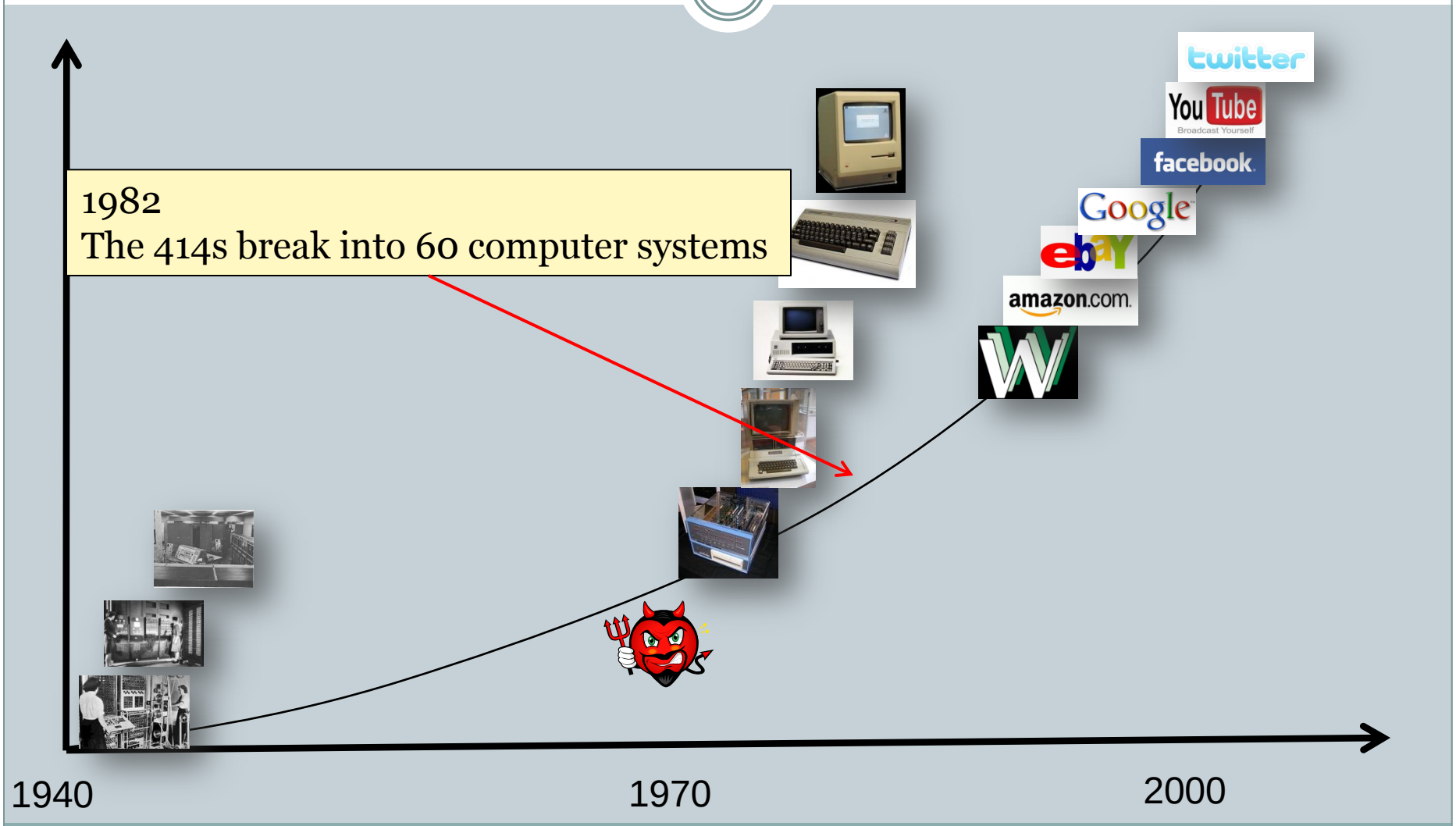


Now looking at computer security…

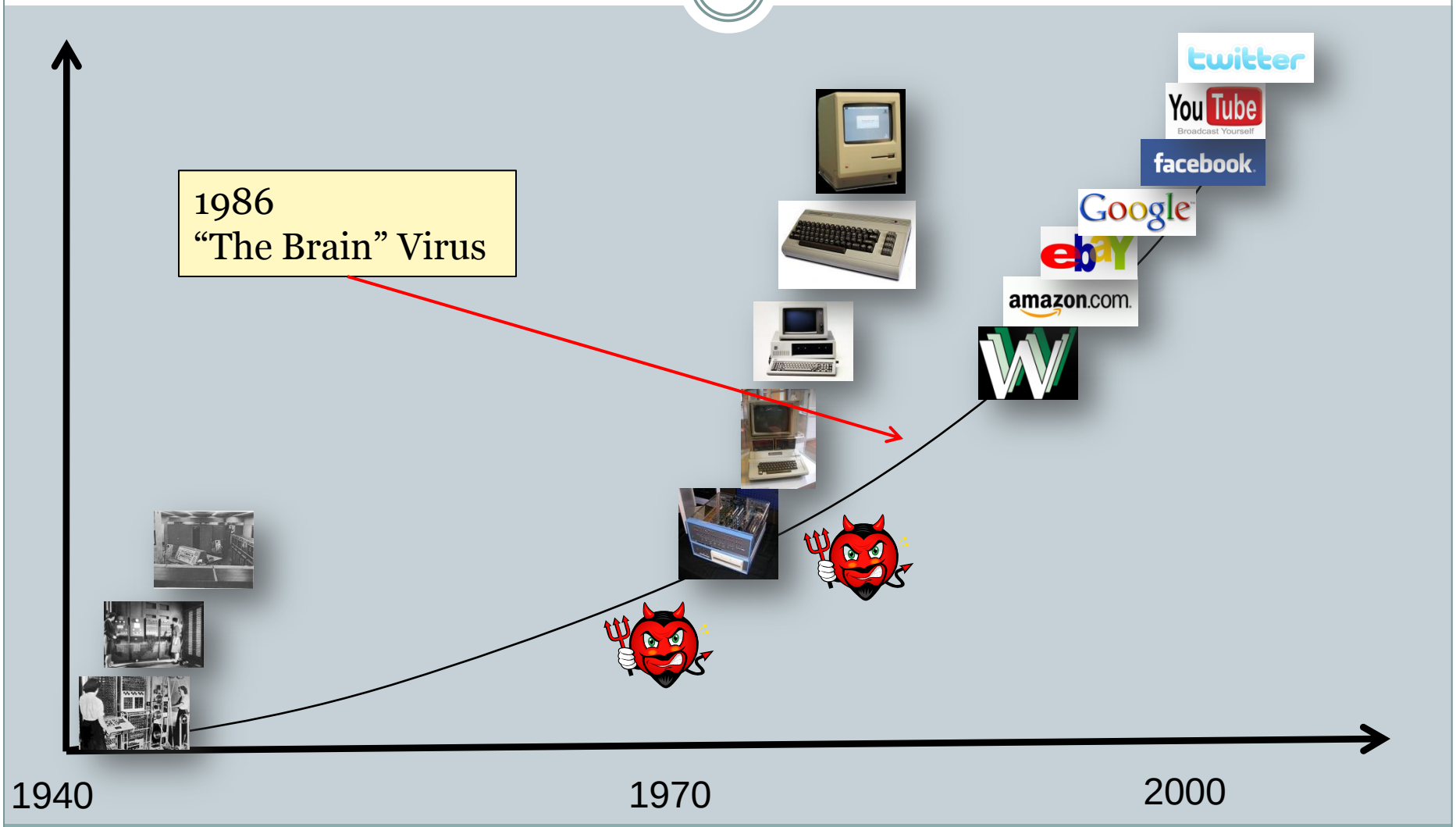
Timeline: Computer Security Attacks



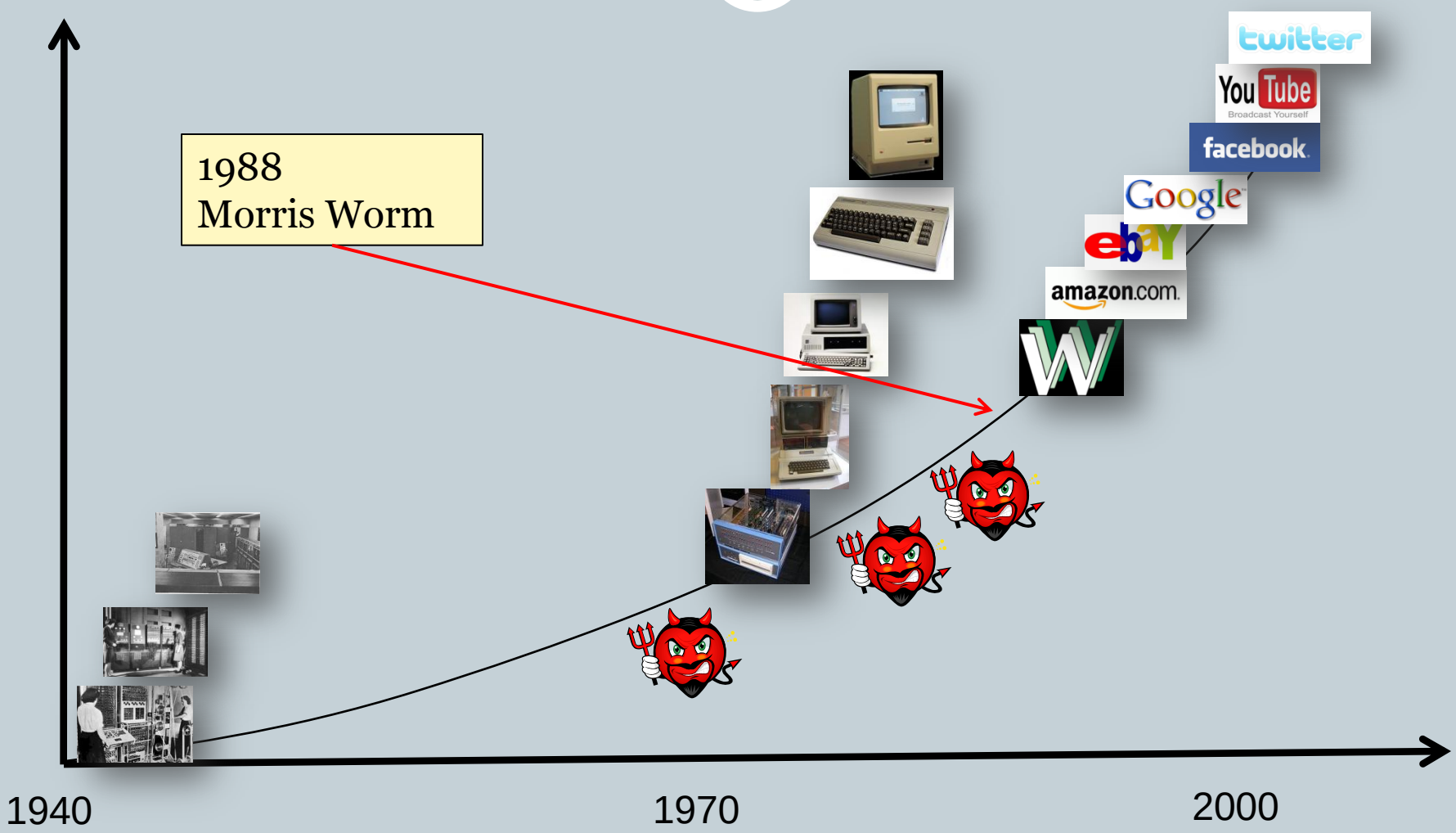
Timeline: Computer Security Attacks



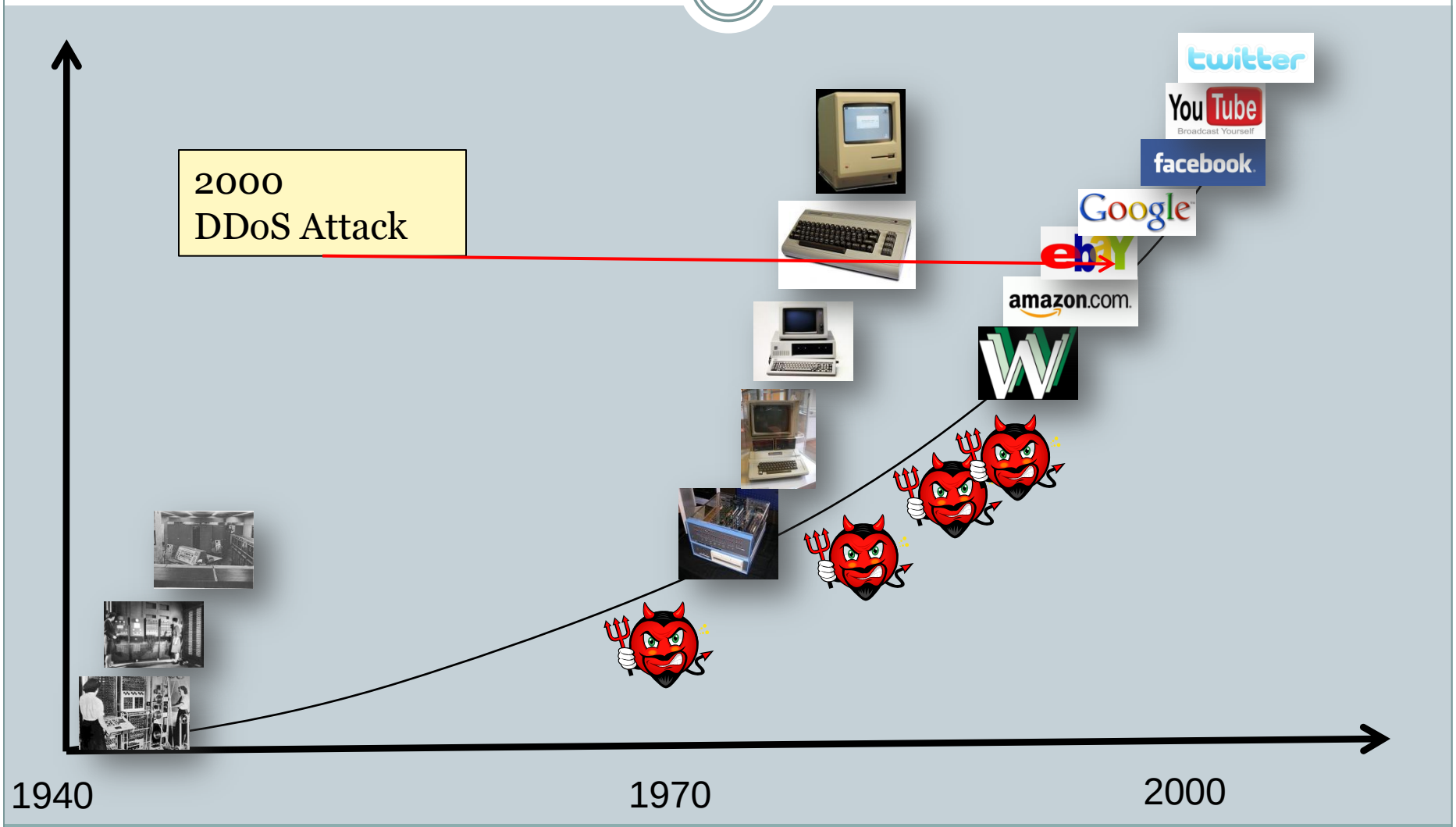
Timeline: Computer Security Attacks



Timeline: Computer Security Attacks

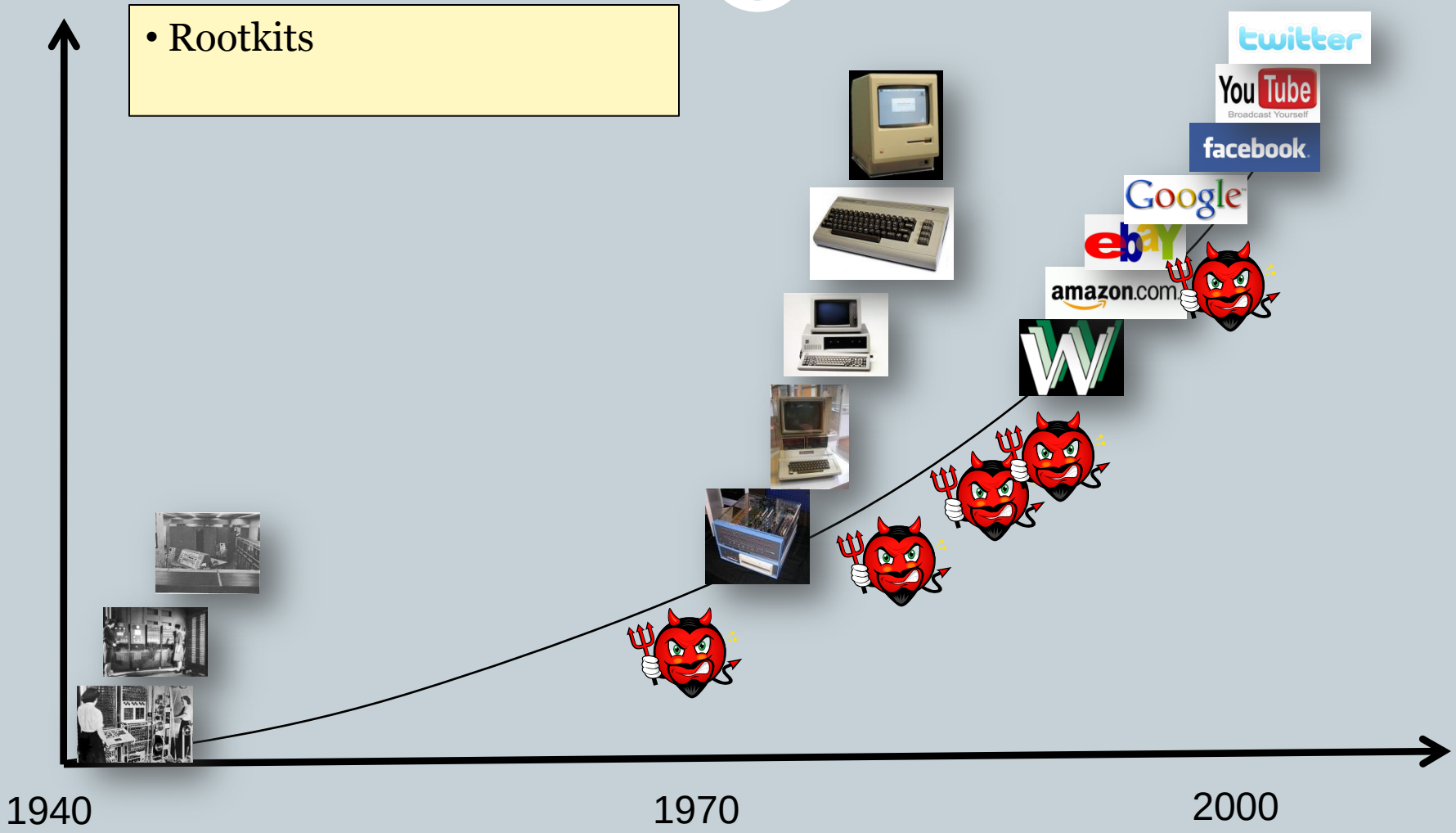


Timeline: Computer Security Attacks



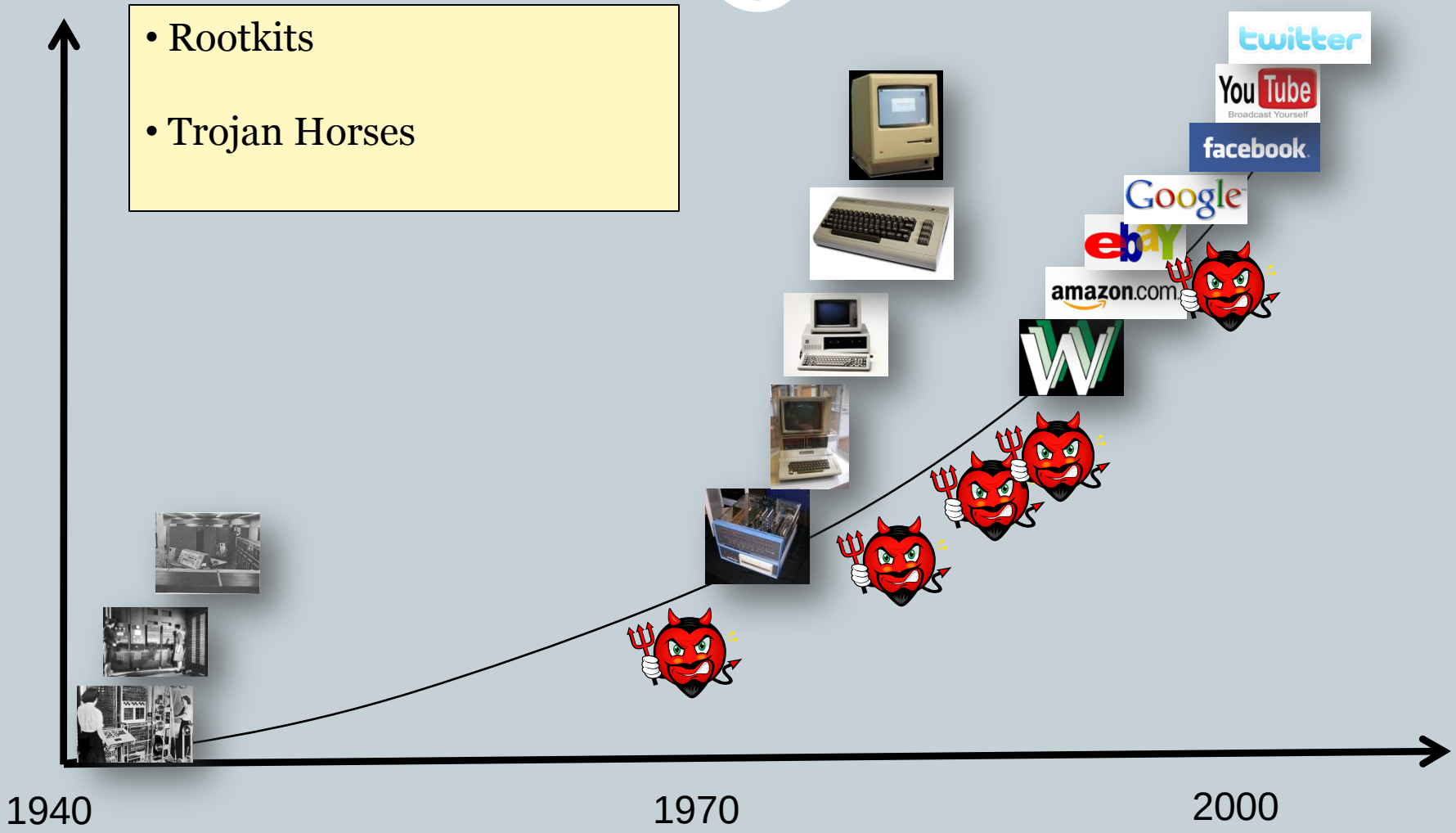
Timeline: Computer Security Attacks

- Rootkits



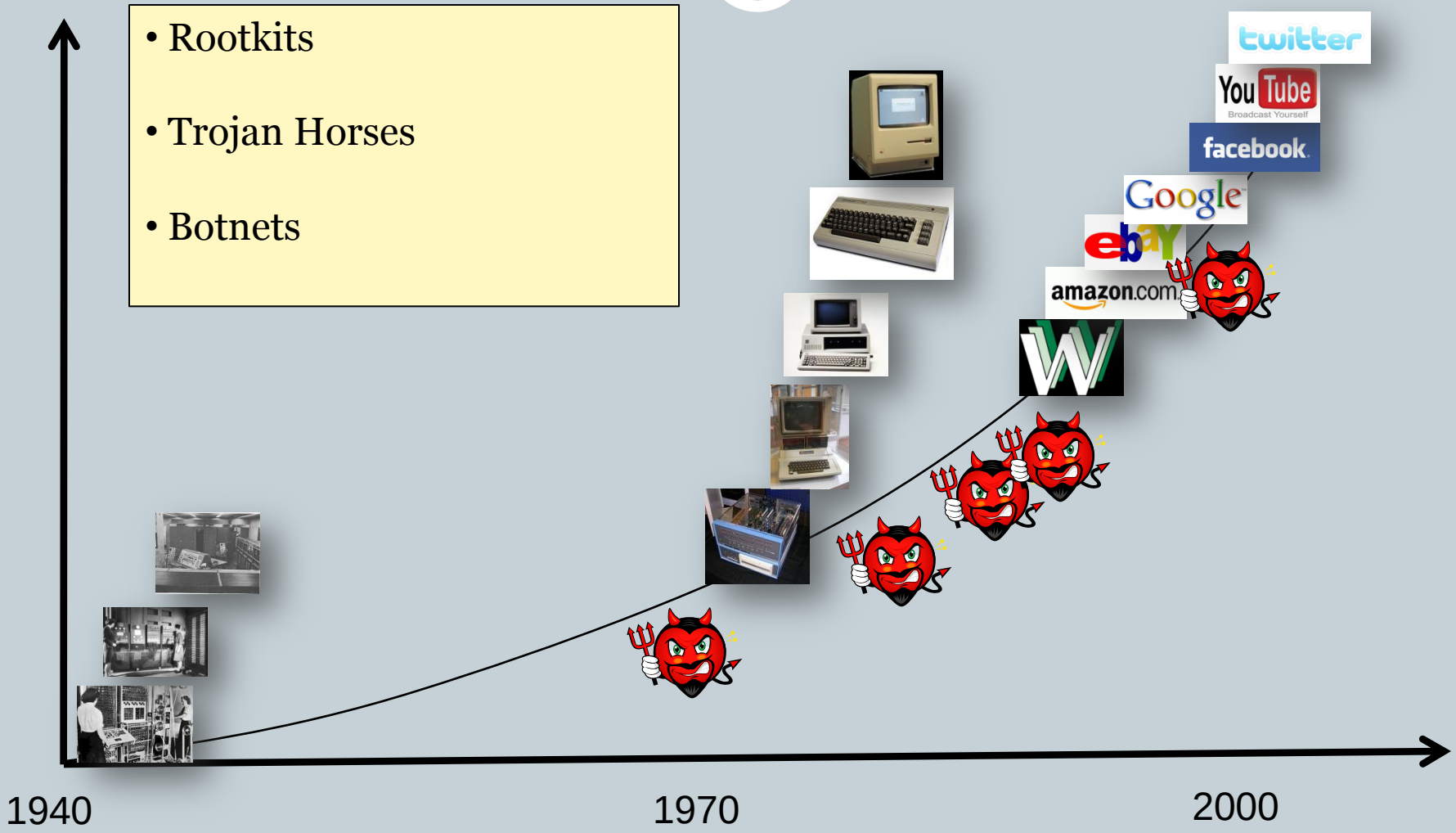
Timeline: Computer Security Attacks

- Rootkits
- Trojan Horses



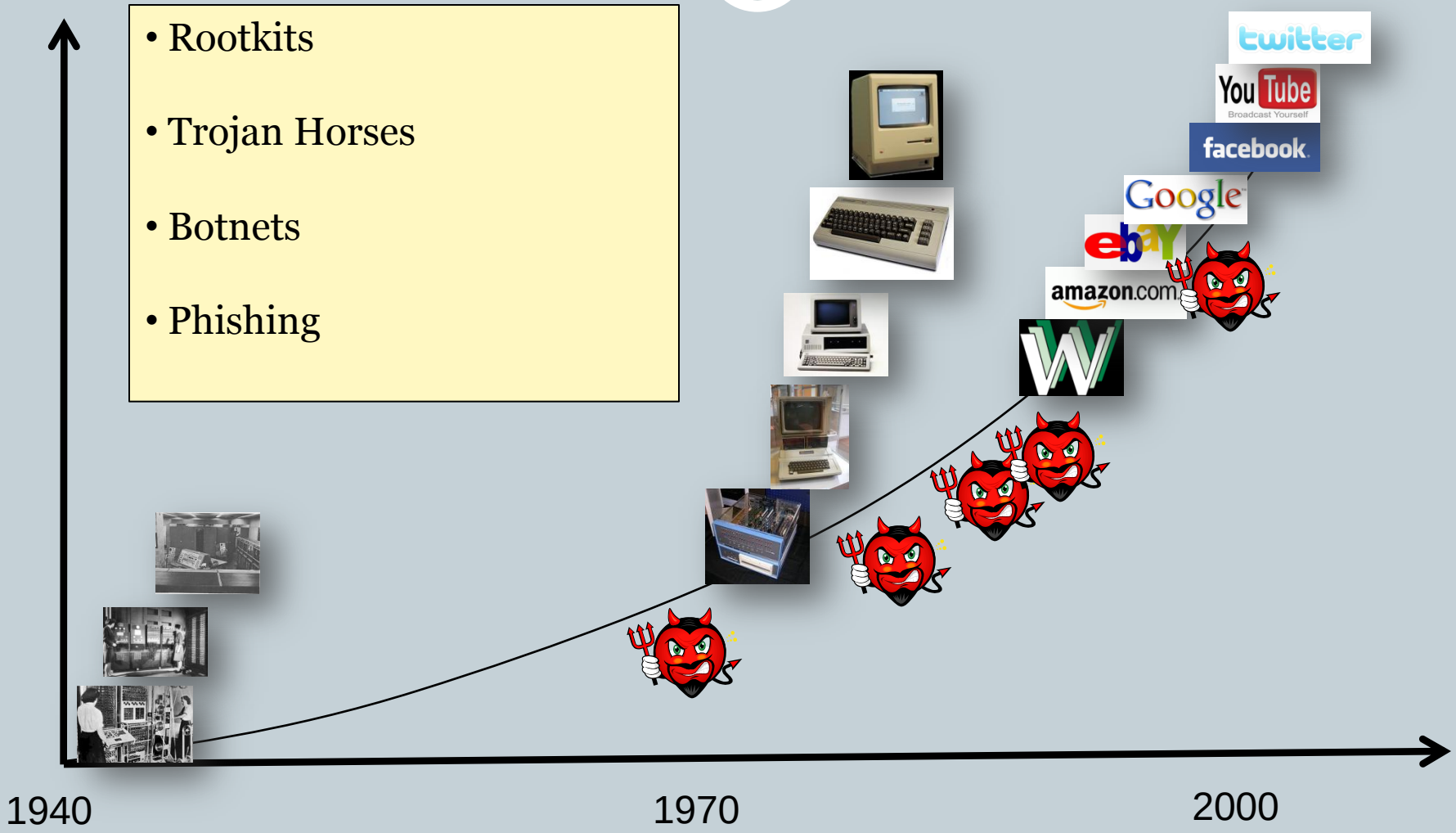
Timeline: Computer Security Attacks

- Rootkits
- Trojan Horses
- Botnets



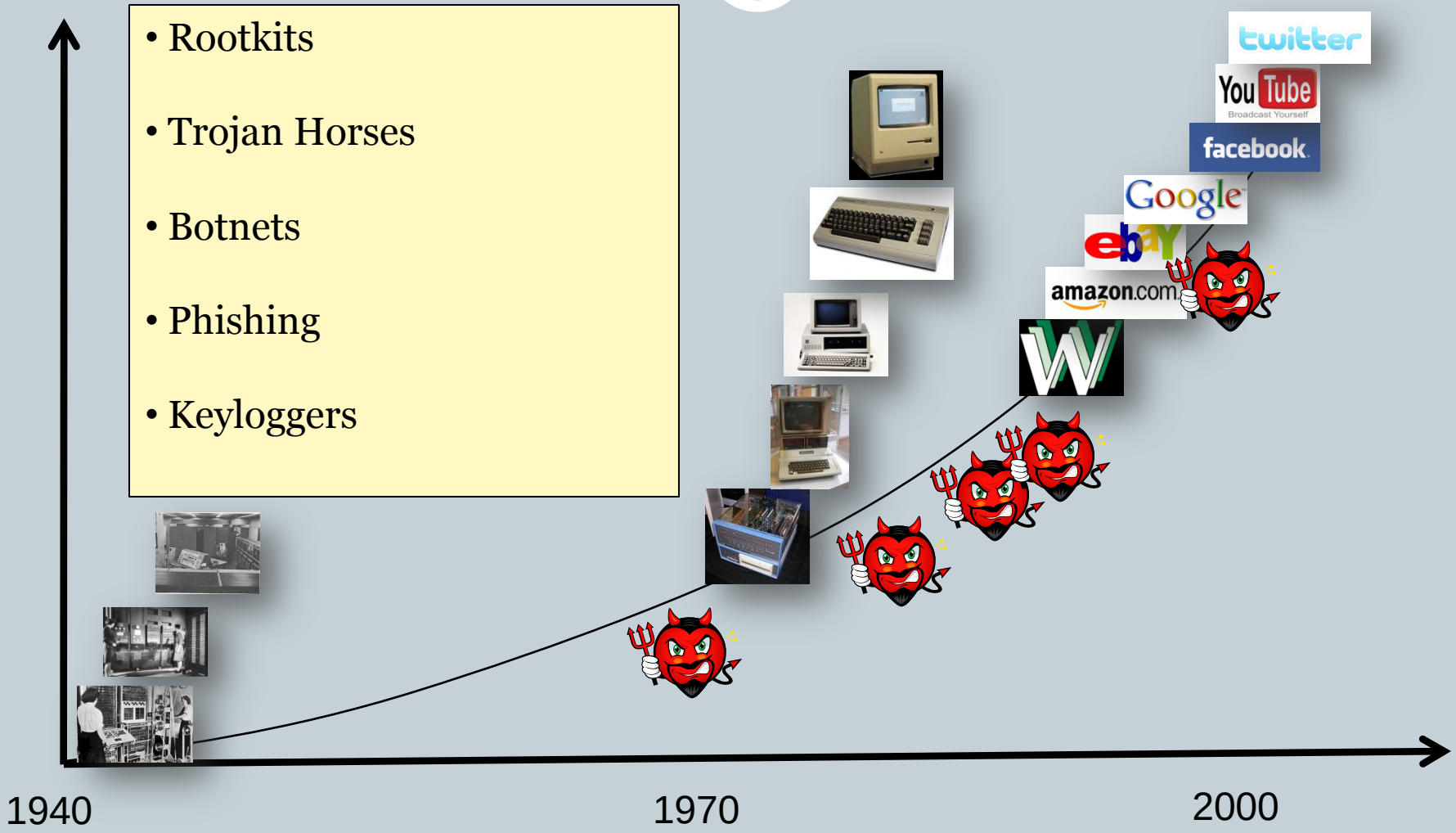
Timeline: Computer Security Attacks

- Rootkits
- Trojan Horses
- Botnets
- Phishing



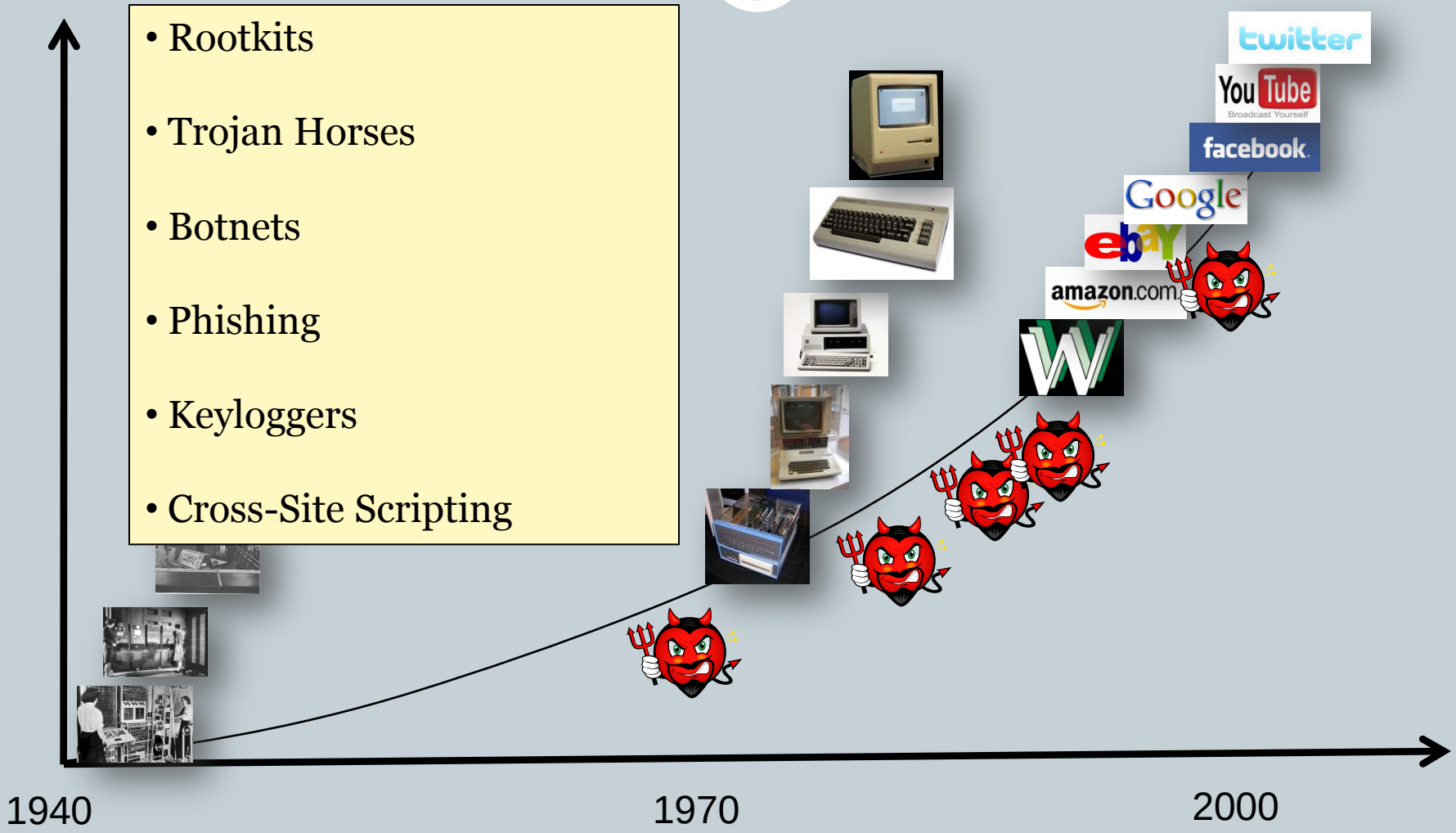
Timeline: Computer Security Attacks

- Rootkits
- Trojan Horses
- Botnets
- Phishing
- Keyloggers



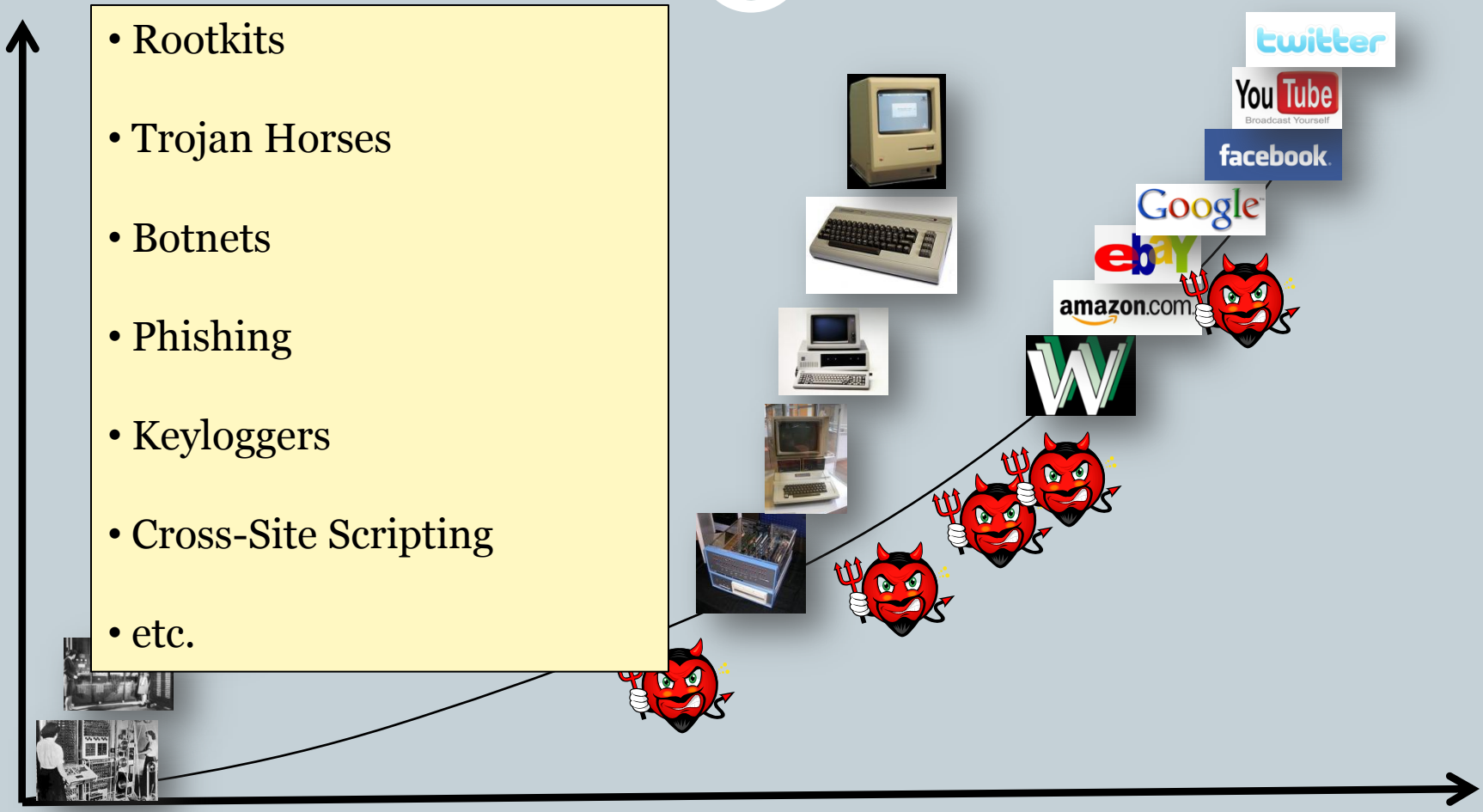
Timeline: Computer Security Attacks

- Rootkits
- Trojan Horses
- Botnets
- Phishing
- Keyloggers
- Cross-Site Scripting



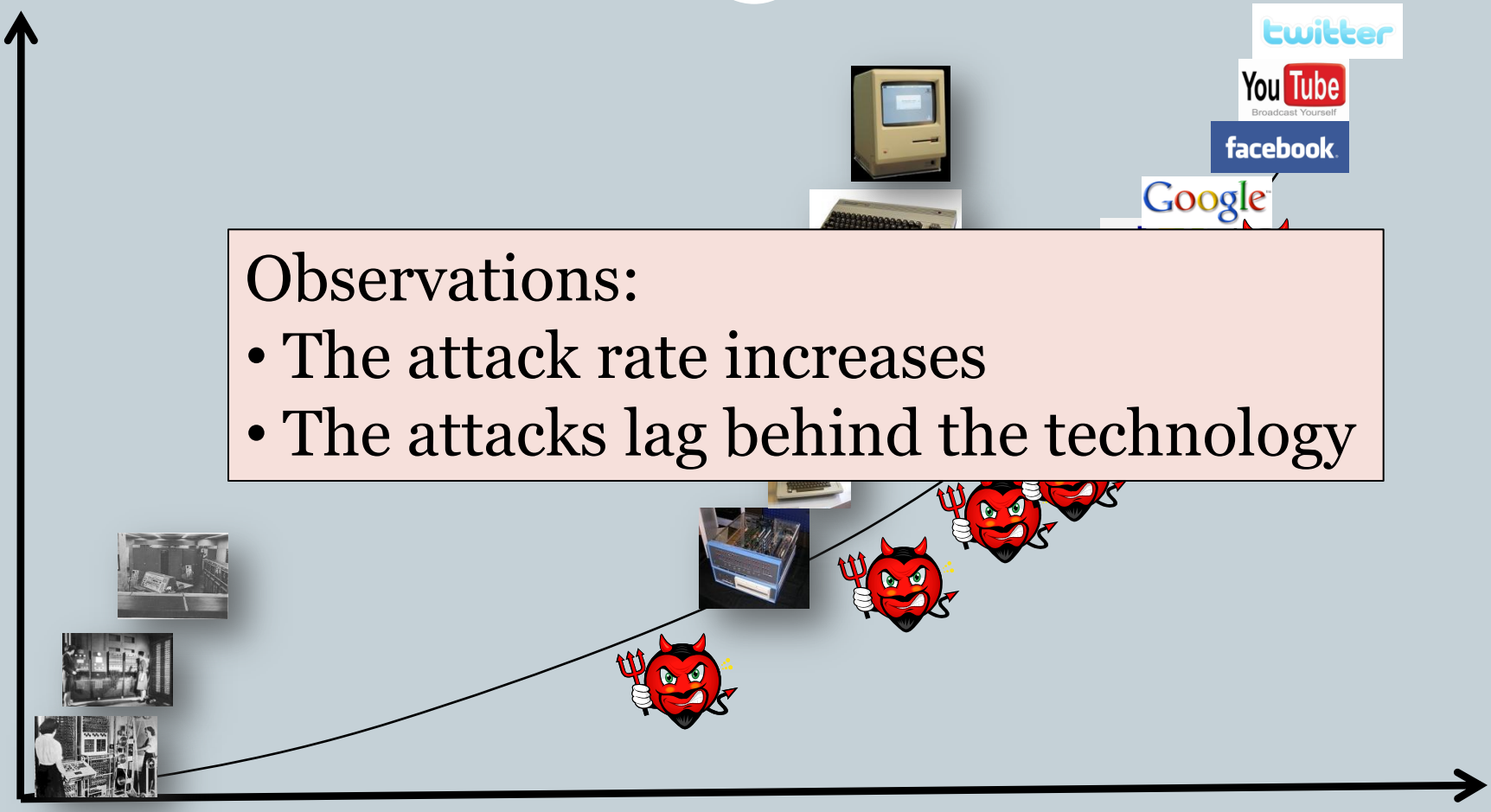
Timeline: Computer Security Attacks

- Rootkits
- Trojan Horses
- Botnets
- Phishing
- Keyloggers
- Cross-Site Scripting
- etc.



1940 1970 2000

Timeline: Computer Security Attacks

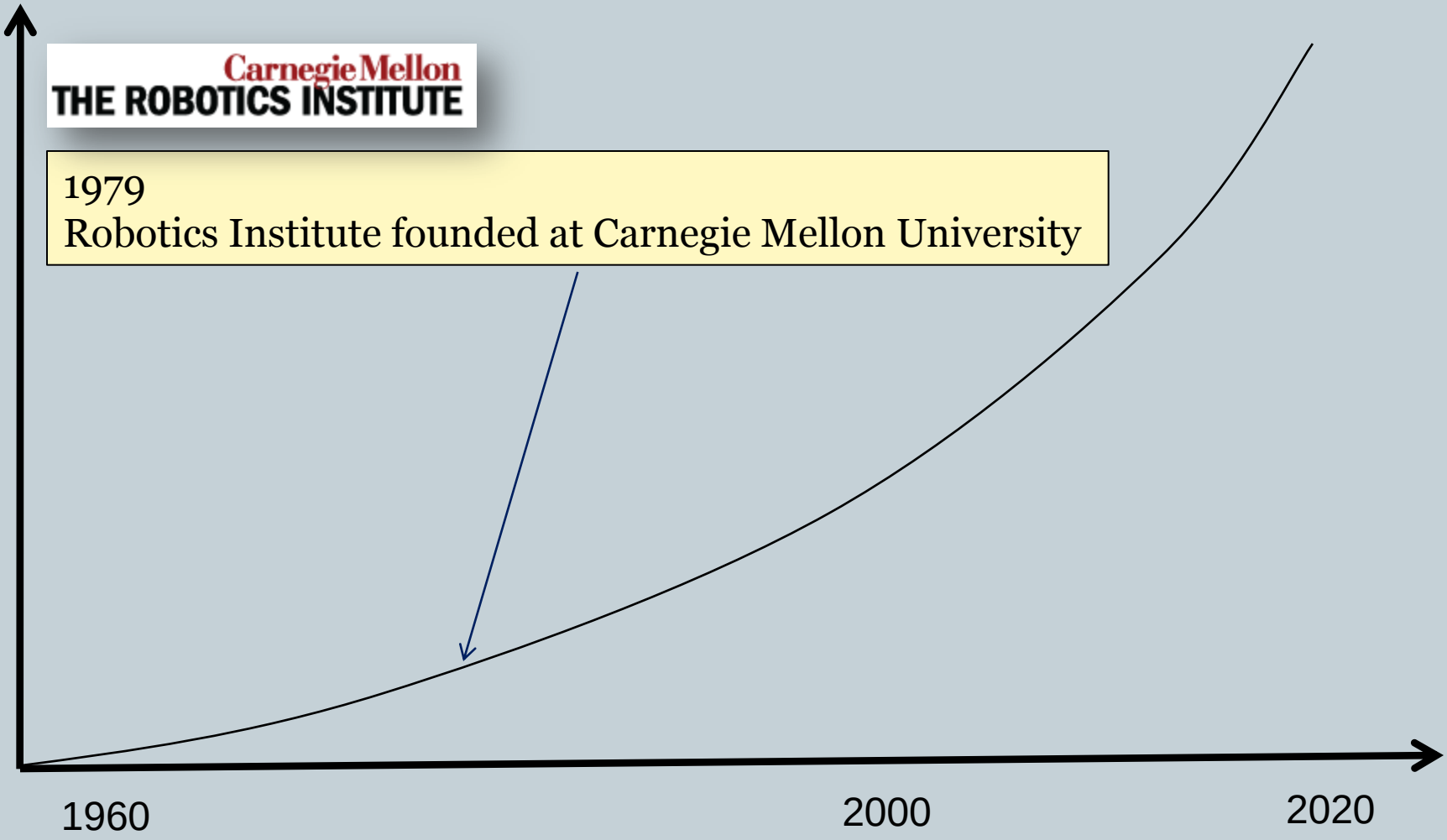


Observations:

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

1940 1970 2000

Timeline: Robots



Timeline: Robots

1982
WABOT-2 accompanies people on a keyboard instrument

Carnegie Mellon
THE ROBOTICS INSTITUTE

1960

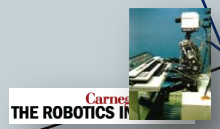
2000

2020

Timeline: Robots

1986
Honda founds Humanoid Robot Division

POWERED by HONDA™



1960 2000 2020

Timeline: Robots

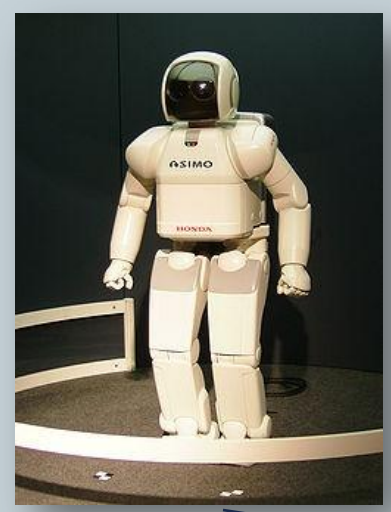
1999
AIBO

1960

2000

2020

Timeline: Robots



2000
ASIMO

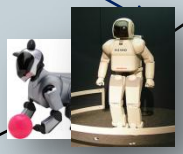
1960

2000

2020

Timeline: Robots

2001
Paro therapeutic seal

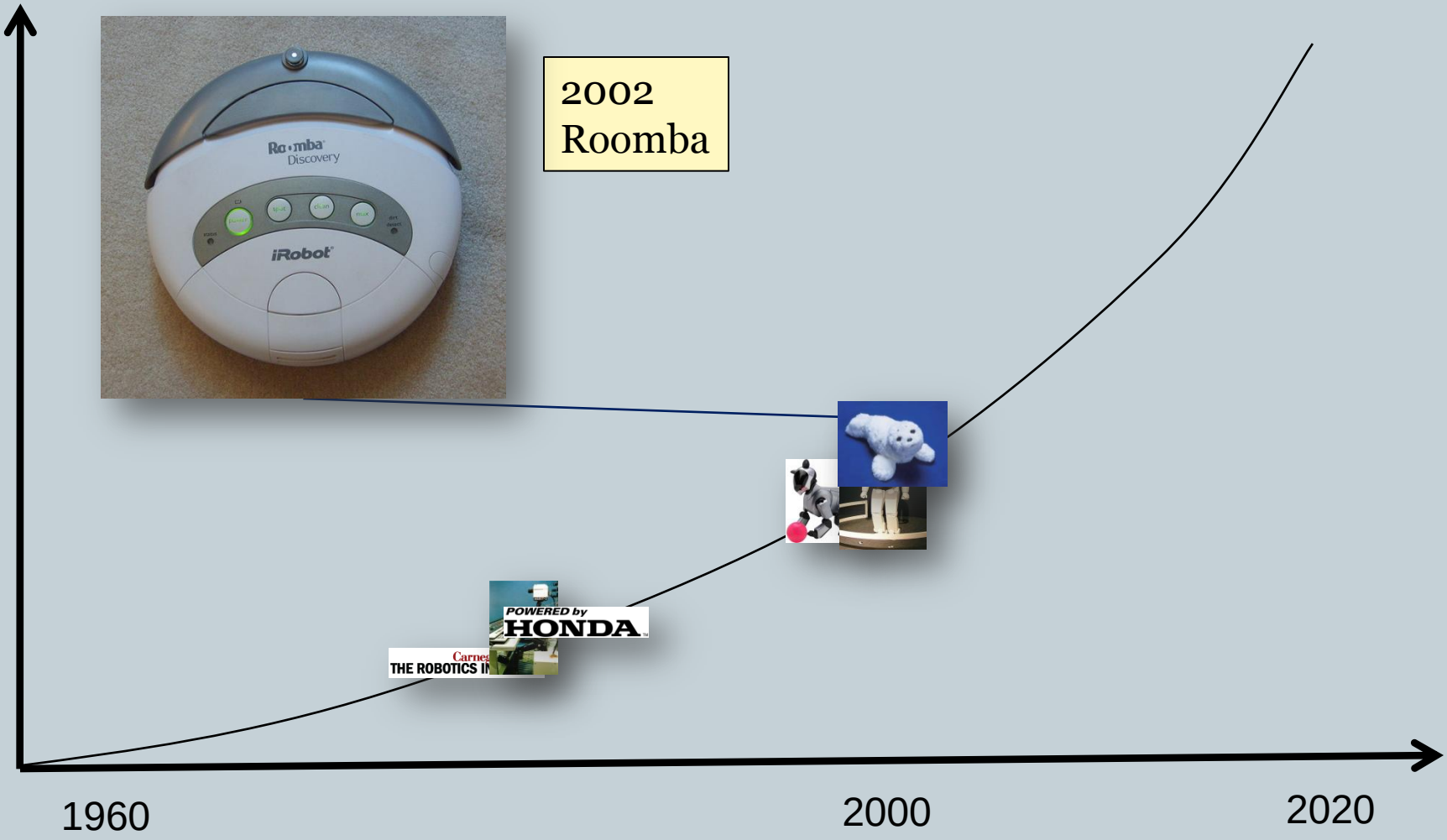


1960

2000

2020

Timeline: Robots



Timeline: Robots

2005
Actroid Android

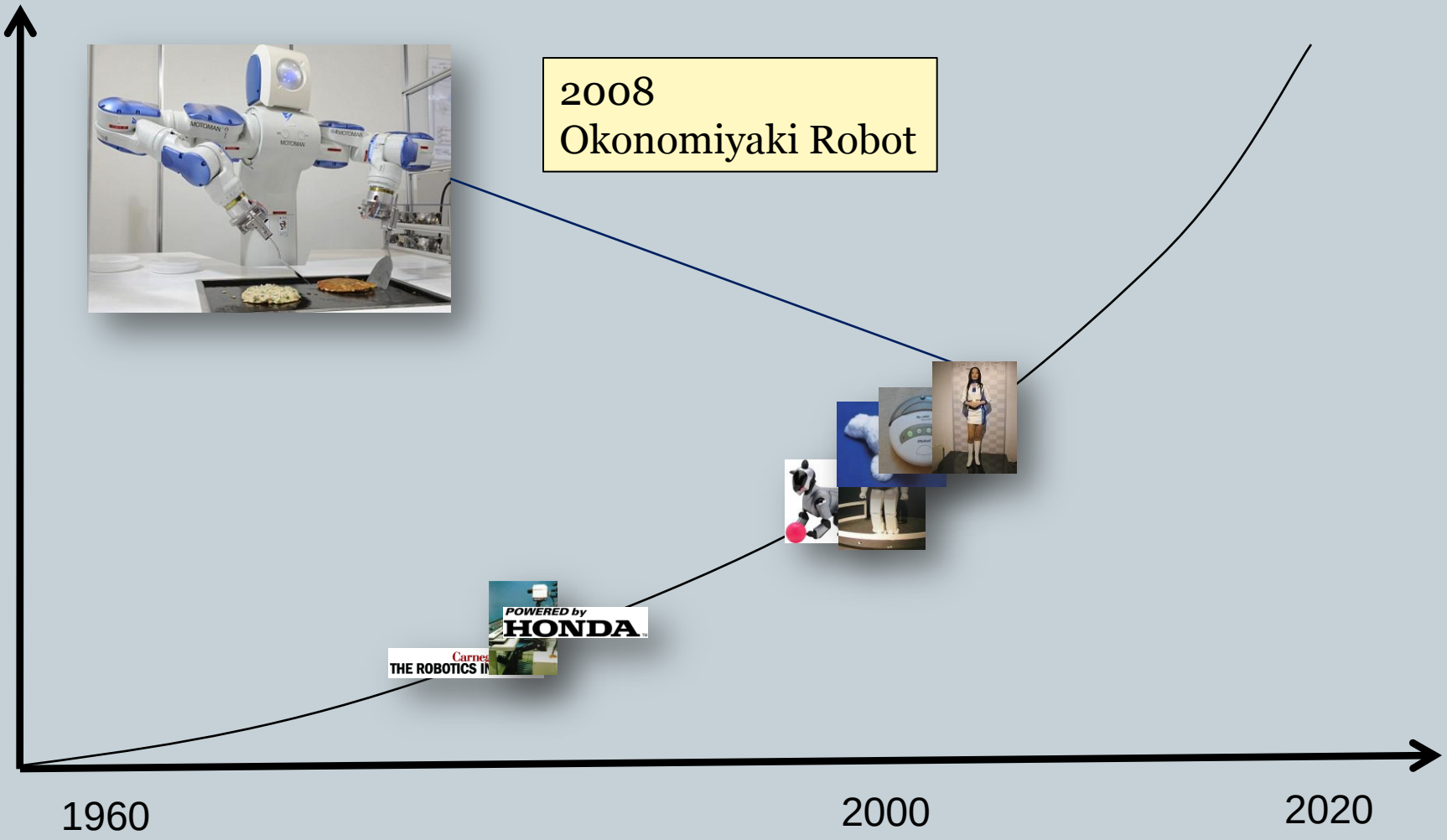
2005
Wakamaru Companion Robot

1960

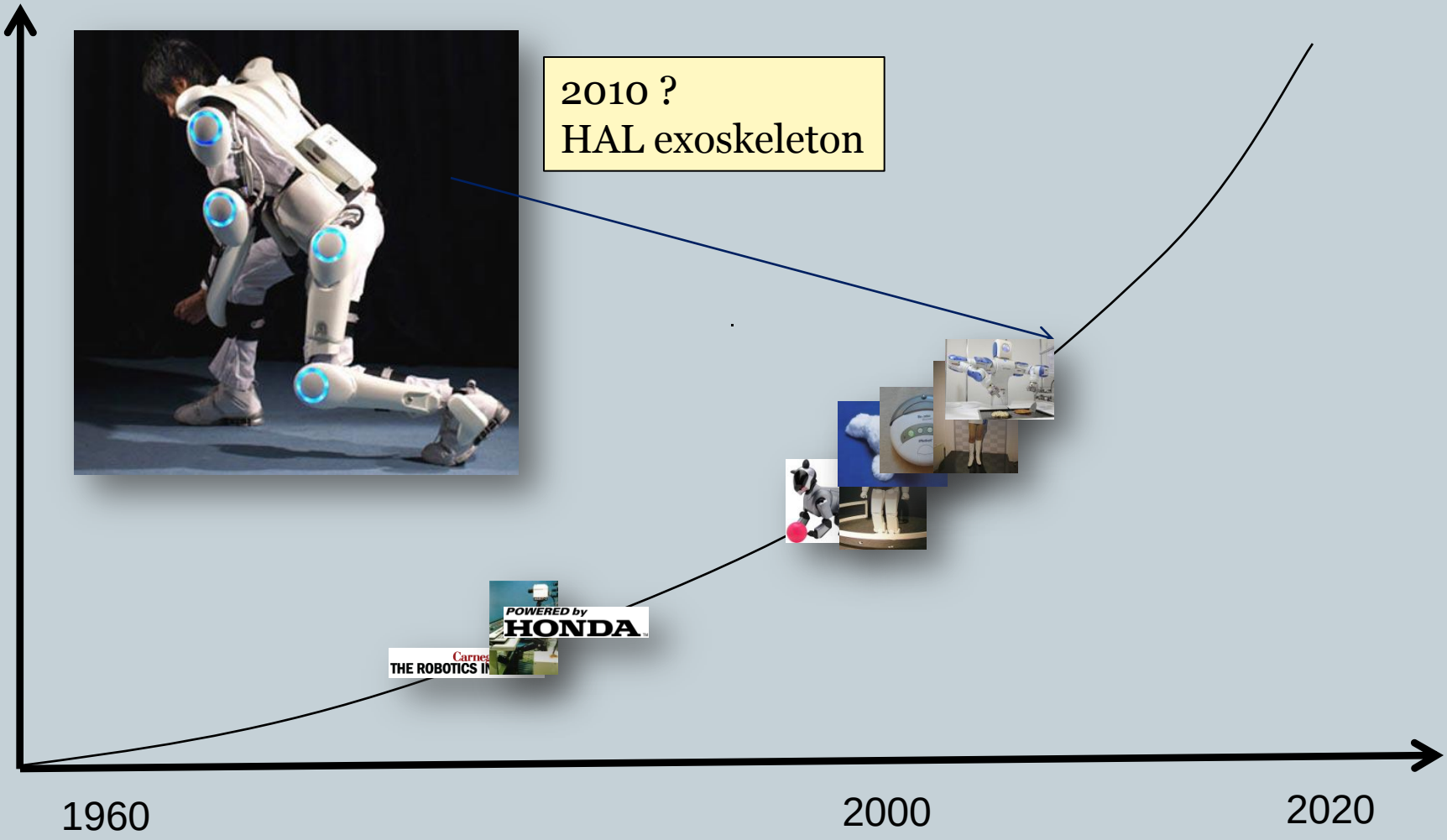
2000

2020

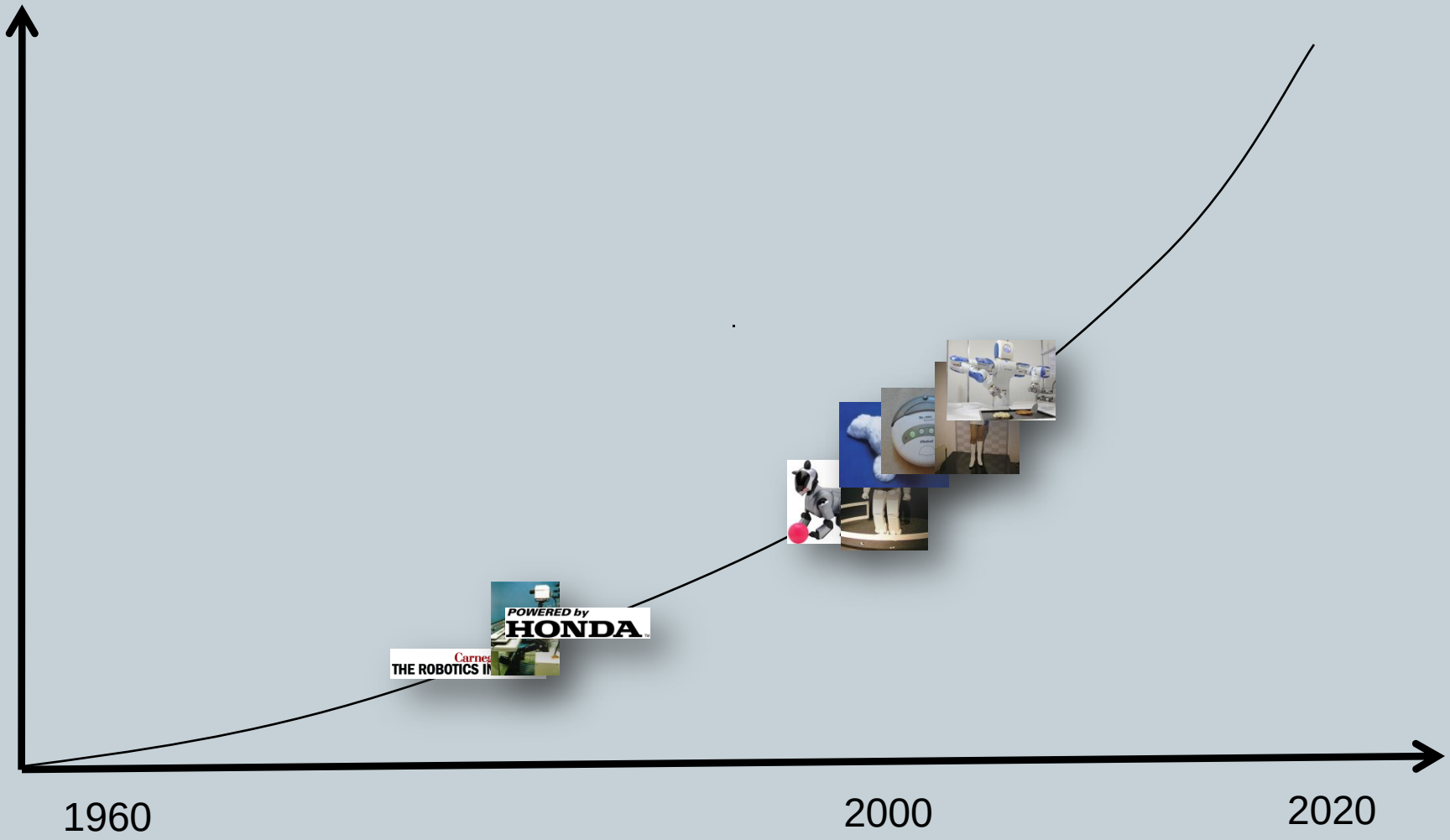
Timeline: Robots



Timeline: Robots



Timeline: Robots



Timeline: Robot Security

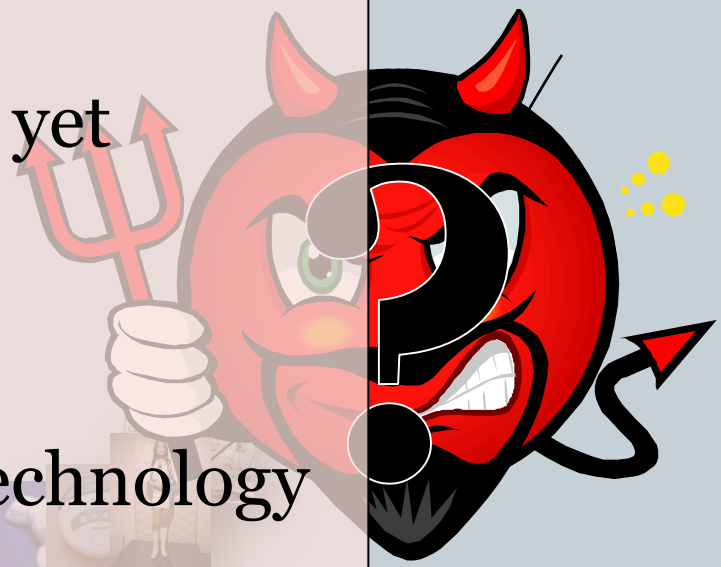
Observation:

- 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?



1960 2000 2020

Robot Security and Privacy in Context

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

Robot Security and Privacy in Context

- 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…

- How to pick which robots to study?

Roomba (vacuum) 	**Scooba (mop)** 	**Robomow (lawn mower)** 
Pleo (artificial lifeform toy) 	**Lego Mindstorm NXT (toy and learning kit)** 	**FlyTech Bladestar (flying toy)** 

Axes for Selecting Representatives Robots

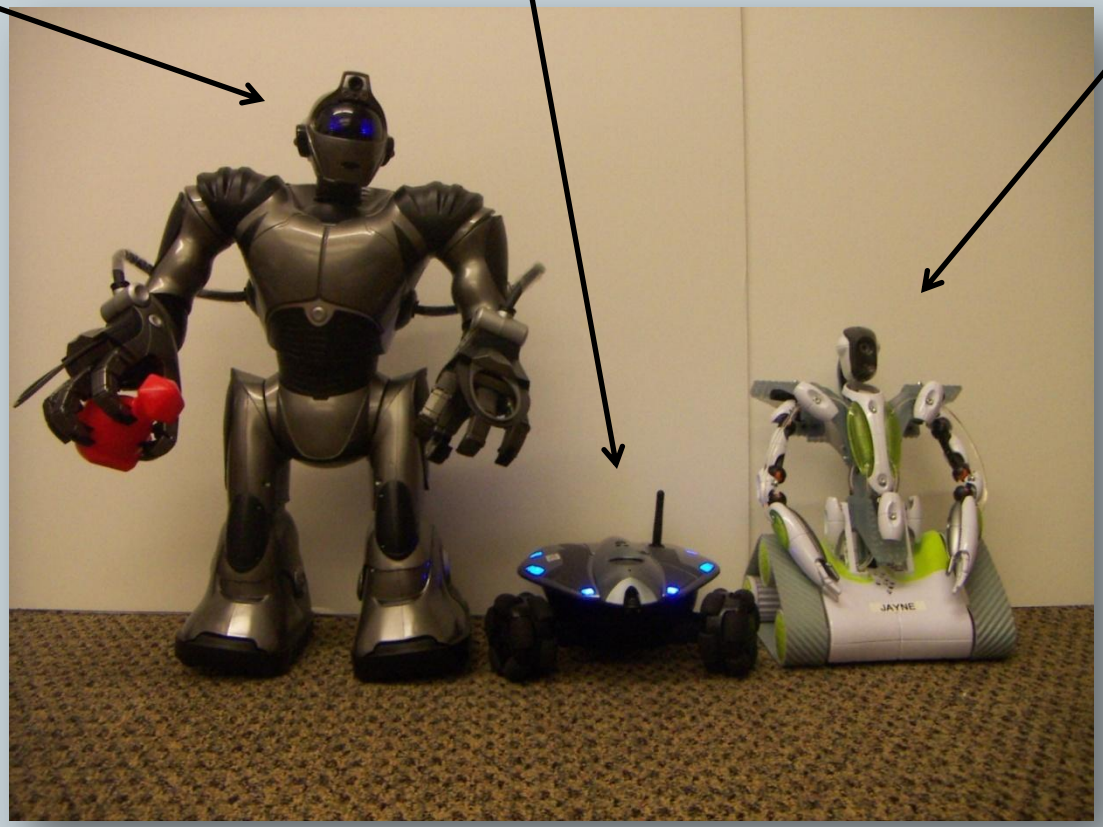
- Strategy: Pick robots that span likely properties of future robots
  - Different Groups of Intended Users
  - Mobility
  - Actuators
  - Sensors
  - Communication Methods

Our Selection: Spanning the Axes

RoboSapien V2

Rovio

Spykee

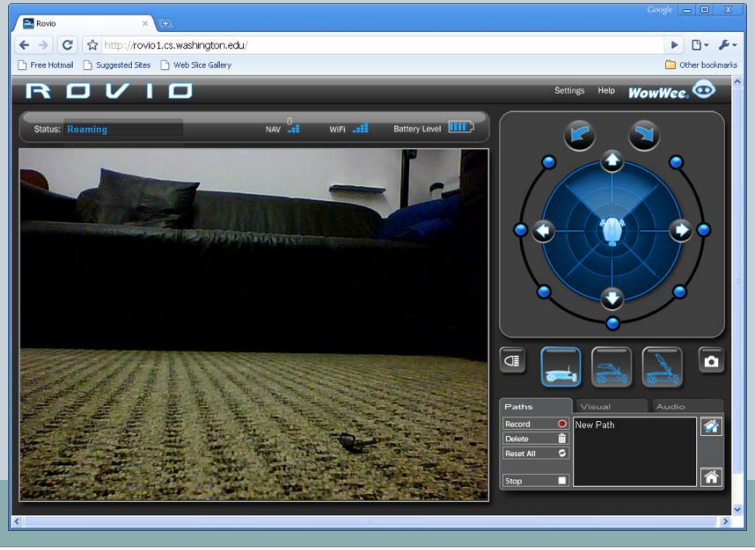


Robots purchased for experimentation during or before October 2008.

RoboSapien V2

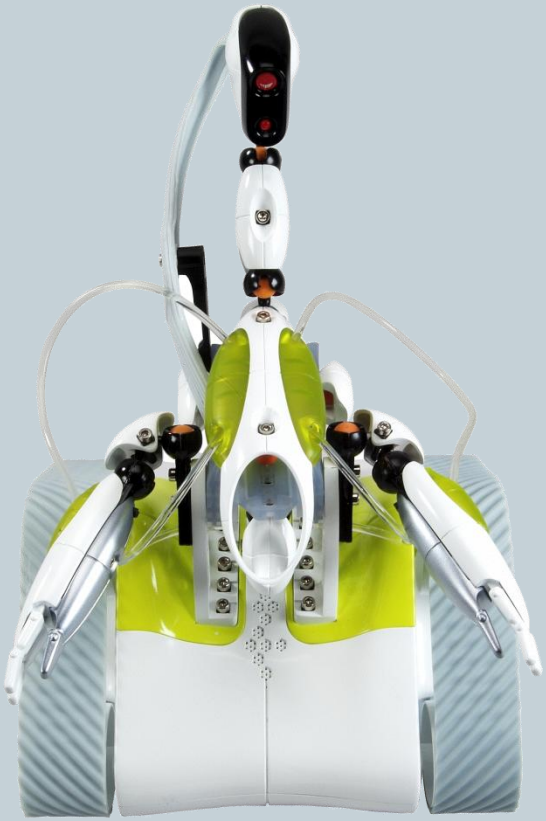
- Toy for children and hobbyists
- Mobile, bipedal
- Basic Dexterity
- Controlled by IR remote
- Some autonomous behavior
- Pre-programmed speech

Rovio



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

Spykee



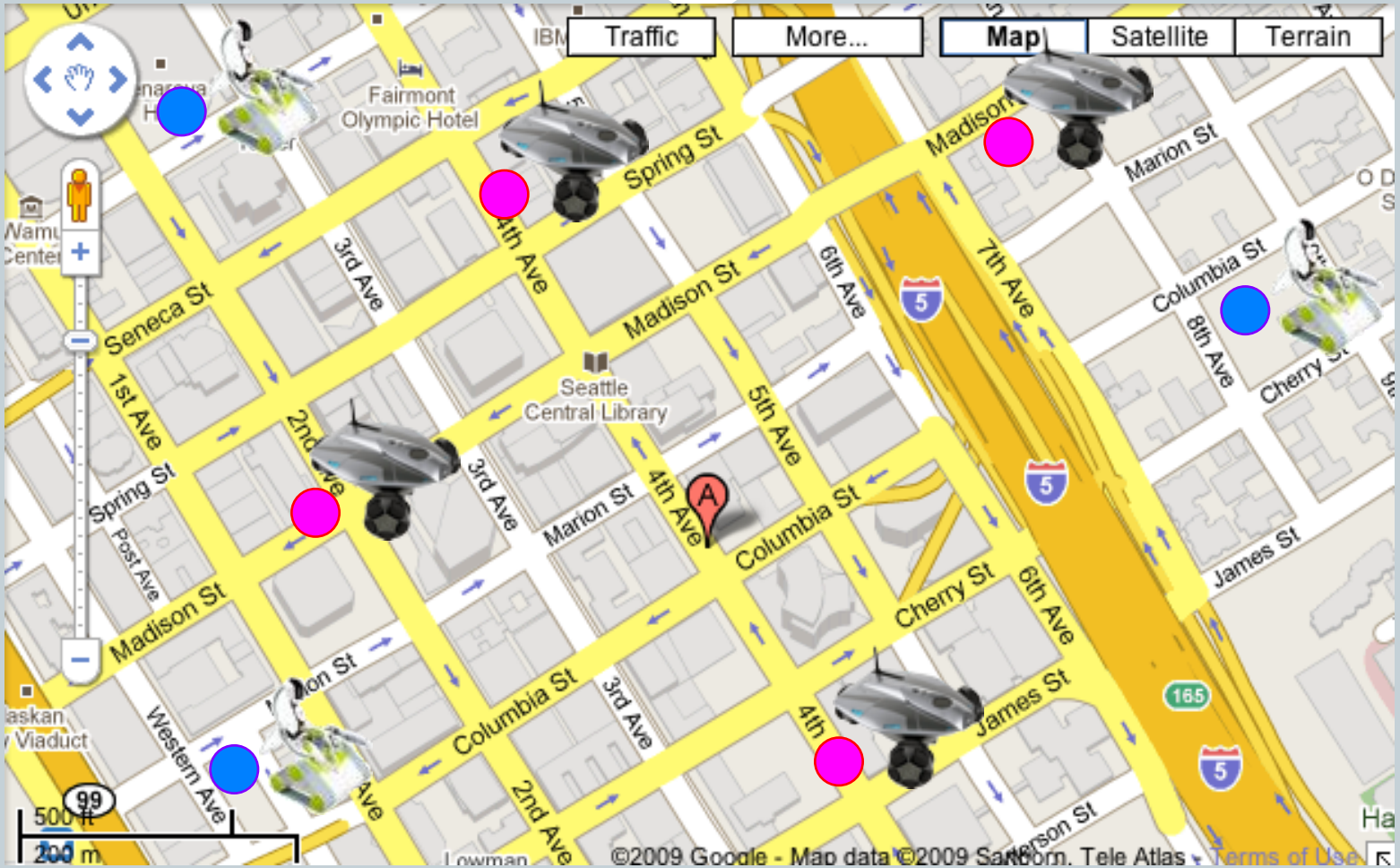
- Toy for children
- Assembled and configured by children
- Telepresence: Parent can tuck in kids when out of town
- “Spy” robot

So, what vulnerabilities did we find?

So, what vulnerabilities did we find?

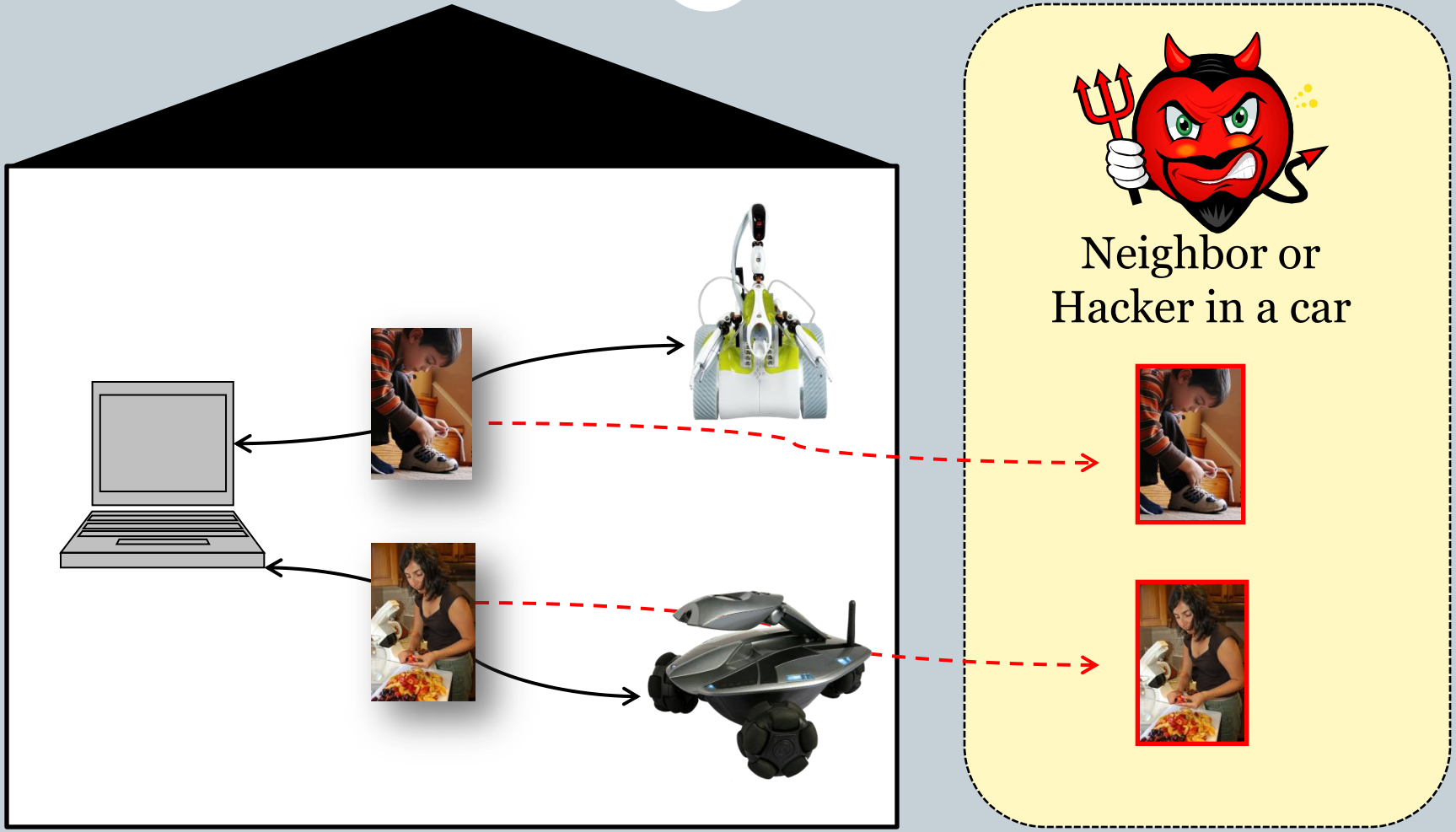
Focusing on Spykee and Rovio for now (we'll come back to RoboSapien V2 later)

Remote Discovery



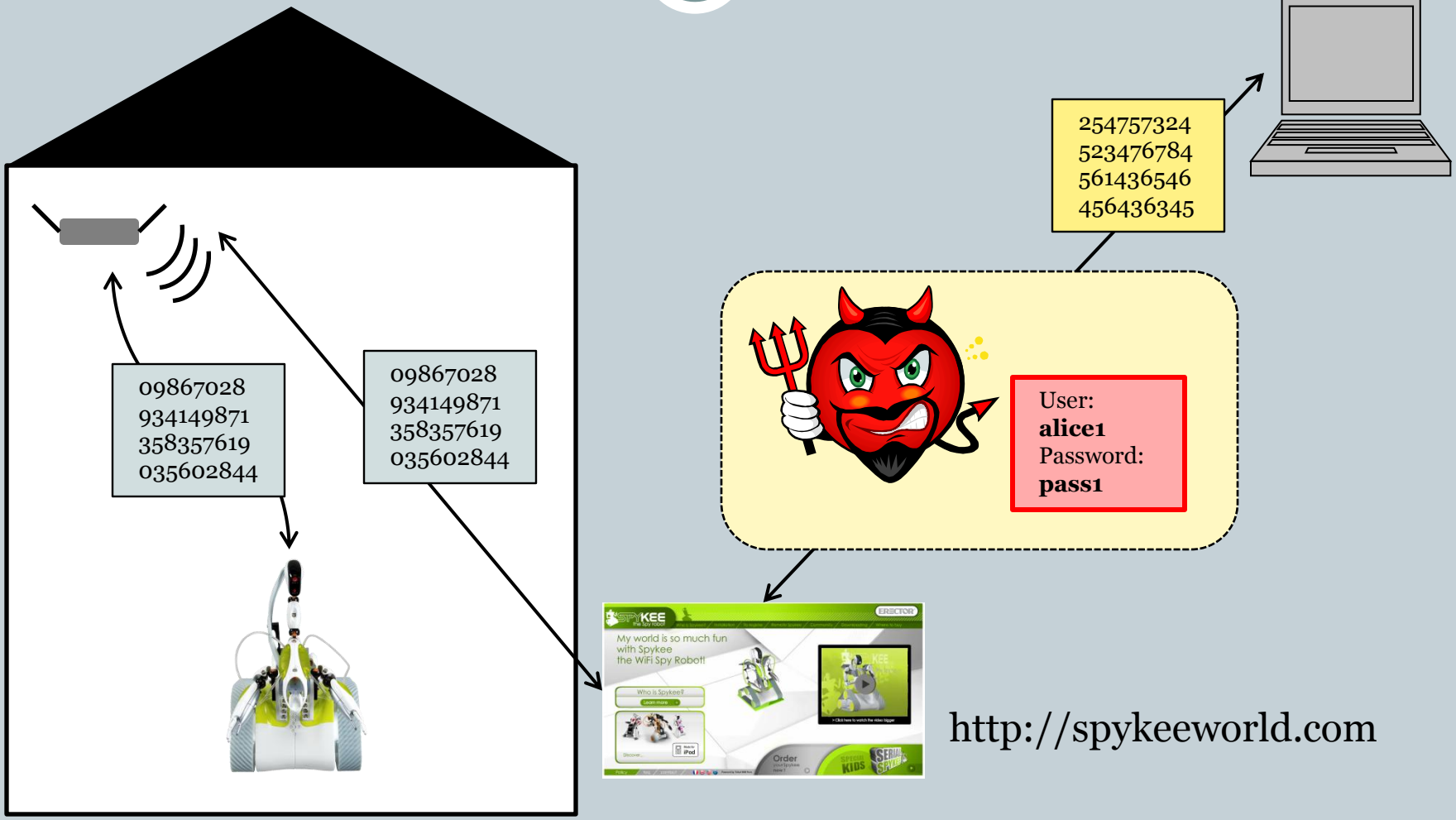
(Artificial data -- not real locations of robots)

Eavesdropping (shown in ad hoc mode)



CC images courtesy of: http://www.flickr.com/photos/wwworks/3039389897/, http://www.flickr.com/photos/jamimages/83601411/

Intercepting Credentials (Remote Mode)



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.

Rovio: Spy on Home

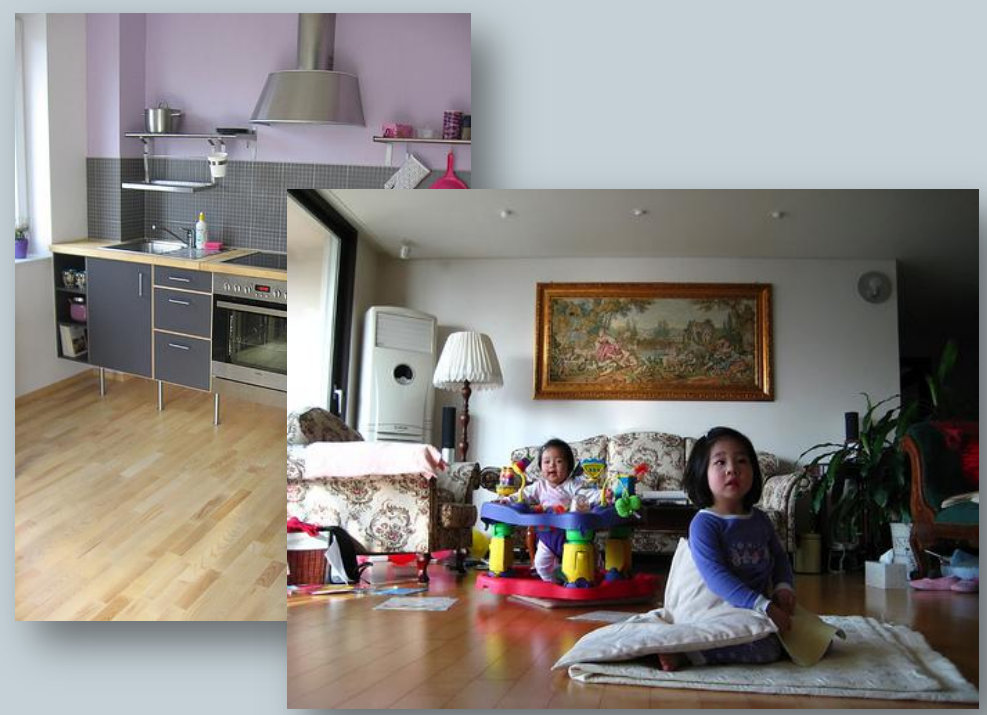
- Spy/eavesdrop in the home

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

CC image courtesy of: http://www.flickr.com/photos/3mieszczanka/3253181023/

Rovio: Spy on Home

- Spy/eavesdrop in the home

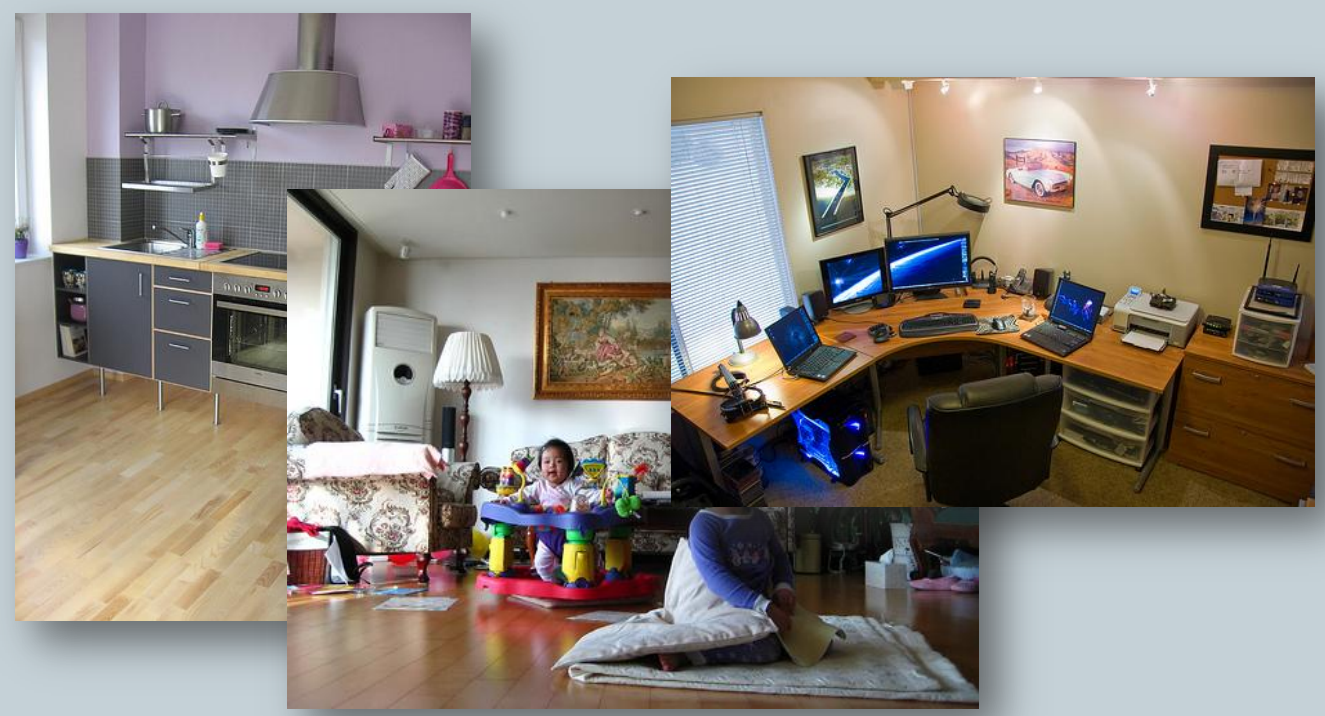


Many risks today are minor. We explore attack scenarios because they illustrate potential future risks with household robots.

CC image courtesy of: http://www.flickr.com/photos/arthurohm/1977354073/

Rovio: Spy on Home

- Spy/eavesdrop in the home

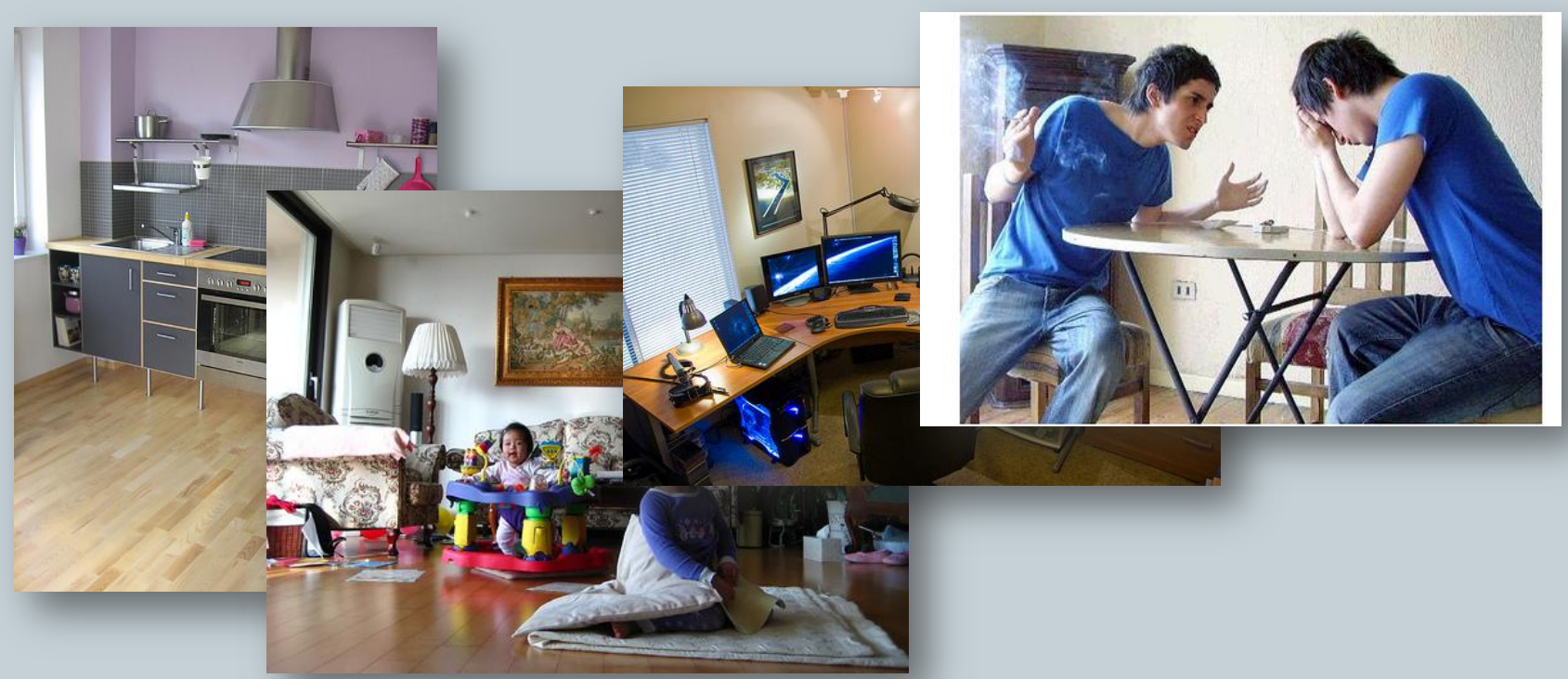


Many risks today are minor. We explore attack scenarios because they illustrate potential future risks with household robots.

CC image courtesy of: http://www.flickr.com/photos/paladin27/2277420652/

Rovio: Spy on Home

- Spy/eavesdrop in the home



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

CC image courtesy of: http://www.flickr.com/photos/affixations/2542167108/

Rovio: Move Around the Home

- 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: Property Damage

- Use weight to cause minor property damage

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

CC image courtesy of: http://www.flickr.com/photos/kacey3/2002598626/

Rovio: Create Hazards

- E.g., Bowl of grapes near an infant

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

CC image courtesy of: http://www.flickr.com/photos/mindfire/3256681195/

Rovio: Trip People

- Drive underneath elder's feet to trip them

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

CC image courtesy of: http://www.flickr.com/photos/marktristan/2733951264/

Rovio: People with Dementia

- 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.

Rovio: Superstitious Symbols

- Create patterns on the floor to play on superstitions

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

Rovio: The Risks

- Spy on residents
- Move between areas of the house to facilitate spying
- Property damage
- Robot suicide
- Knock over objects around infants
- Trip elderly relatives
- Create superstitious symbols

Spykee: The Risks

- Same kinds of risks as the Rovio, but…

Spykee: The Risks

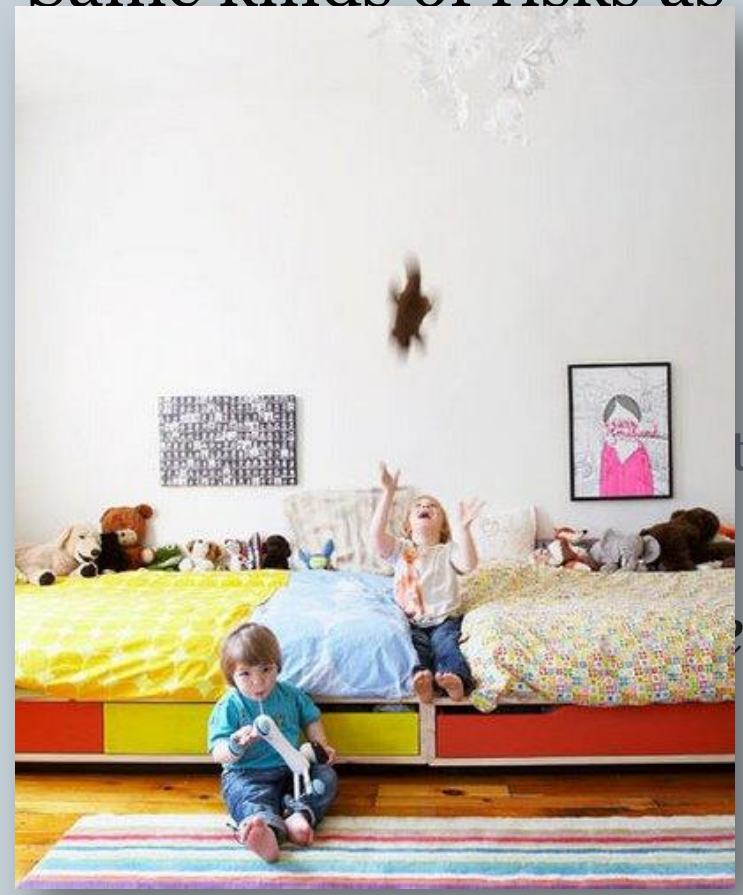
- Same kinds of risks as the Rovio, but…
- Spykee meant to be:
  - Built by children (Erector set, 8+ years)
  - Configured by children
  - Connected to the Internet by children

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…
- t by chi
- *ed wit*



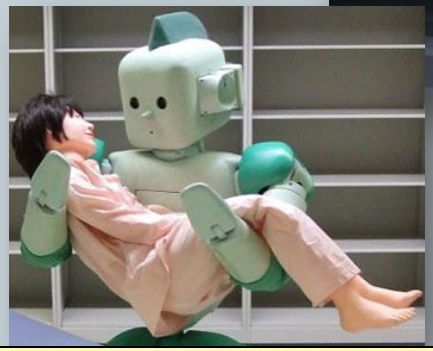
CC images courtesy of: http://www.flickr.com/photos/ooh_food/3510270149/, http://www.flickr.com/photos/aznongbri/945555443/

The Risks Tomorrow

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



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. Th bilities and may or may not be used for attacks. We future kinds of robots.

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

Computer Systems for Physical Harm

Original URL: http://www.theregister.co.uk/2008/01/11/tram_hack/

Polish teen derails tram after hacking train network

By John Leyden
Published Friday 11th January 2008 11:56 GMT

A Polish teenager allegedly turned the tram system in the city of Lodz into his own personal train set, triggering chaos and derailing four vehicles in the process. Twelve people were injured in one of the incidents.

The 14-year-old modified a TV remote control so that it could be used to change track points, *The Telegraph* reports. Local police said the youngster trespassed in tram depots to gather information needed to build the device. The teenager told police that he modified track setting for a prank.

November 2007

PRESS RELEASE

Receive press releases from coping-with-epilepsy.com: By Email **RSS Feeds:** XML MY YAHOO!

Hooligans Attack Epilepsy Patients During Epilepsy Awareness Month

Hooligans attack epilepsy support forum in an attempt to induce seizures amongst the members.

Houston, TX, November 19, 2007 --(PR.com)-- Internet hooligans launched a malicious attack on Coping With Epilepsy (CWE), an internet web site that serves as a peer support network for people with epilepsy, last Saturday. The perpetrators flooded CWE with hateful messages, images of hardcore porn and, worst of all, animated images with rapidly flashing colors in an attempt to induce seizures in the photosensitive members (and guests) of the site.

The attack lasted several hours as CWE moderators, many of them photosensitive themselves, battled to remove the offensive content as fast as it was being posted. The attack ended when CWE administrators arrived and locked down the site.

"I was able to trace back the source of the attack to a handful of sites where the perpetrators were instigating the event," said

"It was just a bunch of very immature people delighting in their attempts to cause people misery"

popularity of the site. We're working to ensure that there will never be a repeat performance."

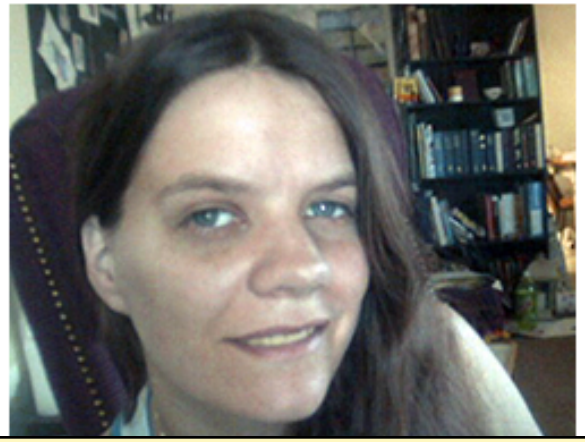
Ironically, the attack occurred during November, which is National Epilepsy Awareness Month.

About CWE
Coping With Epilepsy is a peer support forum for people living with epilepsy. It boasts a world-wide membership including medical professionals.

Again in March 2008

Hackers Assault Epilepsy Patients via Computer

By Kevin Poulsen 03.28.08 | 8:00 PM



Internet griefers descended on an epilepsy support message board last weekend and used JavaScript code and flashing computer animation to trigger migraine headaches and seizures in some users.

The nonprofit Epilepsy Foundation, which runs the forum, briefly closed the site Sunday to purge the offending messages and to boost security.

"We are seeing people affected," says Ken Lowenberg, senior director of web and print publishing at the Epilepsy

"This was clearly an act of vandalism with the intent to harm people"

The attackers turned to a more effective tactic on Sunday, injecting JavaScript into some posts that redirected users' browsers to a page with a more complex image designed to trigger seizures in both photosensitive and pattern-sensitive epileptics.

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

No Longer a Desktop Computer: New Challenges

- Even if you secure one robot in isolation…

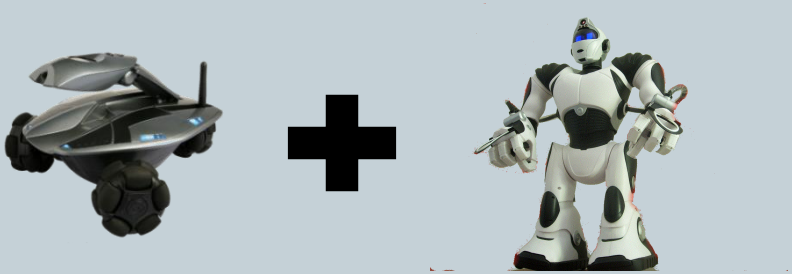
Multi-Robot

- 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

	Rovio 	**RoboSapien V2** 	**IR/RF Repeater**	**Combined**
AV Feed	✖			✖
Grippers		✖		✖
Communication Out of Line of Sight	✖		✖	✖

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

Related Work

- Challenges with ubiquitous computing in the home, e.g.:
  - Edwards and Grinter. “At Home with Ubiquitous Computing: Seven Challenges.” UbiComp ‘01.
- Human-robot interaction in the home, e.g.:
  - Young *et al*. “Toward Acceptable Domestic Robots: Applying Insights from Social Psychology.” Intl. Journal of Social Robotics ‘08.
- Privacy leaks in the home, e.g.:
  - J. Schwartz. “Nanny-Cam May Leave a Home Exposed.” The New York Times, April 2002.
- Usable Security, e.g.:
  - Bryan D. Payne, W. Keith Edwards, "A Brief Introduction to Usable Security," IEEE Internet Computing, vol. 12, no. 3,

Questions?