Security metrics: is this even possible?

Xenia Mountrouidou (Dr. X)
Why security metrics?
To measure is to know.
If you cannot measure it, you cannot improve it.
- Lord Kelvin
**GUIDE TO CONVERTING TO METRIC**

**TEMPERATURE**
- 60°C: Earth's hottest
- 45°C: Dubai heat wave
- 40°C: Southern US heat wave
- 35°C: Northern US heat wave
- 30°C: Beach weather
- 25°C: Warm room
- 20°C: Room temperature
- 10°C: Jacket weather
- 0°C: Snow!
- -5°C: Cold day (Boston)
- -10°C: Cold day (Moscow)
- -20°C: Cold day (Tokyo)
- -30°C: Cold day (Moscott)
- -40°C: Spits goes "cunk!"

**THE KEY TO CONVERTING TO METRIC IS ESTABLISHING NEW REFERENCE POINTS. WHEN YOU HEAR “68°”, INSTEAD OF THINKING “THAT'S 79°”, YOU SHOULD THINK, “THAT'S WARMER THAN A HOUSE BUT COOL FOR SWIMMING.” HERE ARE SOME HELPFUL POINTS OF REFERENCE:**

**LENGTH**
- 1 cm: Width of MicroSD card
- 3 cm: Length of SD card
- 12 cm: CD diameter
- 14 cm: Long pen
- 80 cm: Doorway width
- 1 m: Lightsaber blade
- 170 cm: Summer Guay
- 200 cm: Darth Vader
- 2.5 m: Ceiling
- 5 m: Car-length
- 16 m: Human tower of Serenity crew

**SPEED**
- 1 km/h: Walking
- 13 km/h: Running
- 25 km/h: Sprinting
- 10 km/h: Fastest human
- 13 km/h: Housecat
- 15 km/h: Rabbit
- 1 km/h: Rapper
- 10 km/h: Slow highway
- 100 km/h: Interstate (65 mph)
- 120 km/h: Speed you actually go when it says 65
- 140 km/h: Rapper on hoverboard

**VOLUME**
- 3 L: Blood in a fieldmouse
- 5 mL: Teaspoon
- 30 mL: Nasal passages
- 40 mL: Shot glass
- 350 mL: Soda can
- 350 mL: Water bottle
- 1 L: Jugulator bottle
- 5 L: Blood in human male
- 30 L: Milk crate
- 55 L: Summer Guay
- 65 L: Dennis Kucinich
- 75 L: Ron Paul
- 200 L: Fridge

**MASS**
- 3 g: Peanut M&M
- 100 g: Cell phone
- 500 g: Bottled water
- 1 kg: Ultralight laptop
- 2 kg: Light-medium laptop
- 3 kg: Heavy laptop
- 5 kg: LCD monitor
- 15 kg: CRT monitor
- 4 kg: Cat
- 11 kg: Cat (with captions)
- 60 kg: Lady
- 70 kg: Dude
- 150 kg: Shaq
- 200 kg: Your mom
- 220 kg: Your mom (incl. cheap jewelry)
- 235 kg: Your mom (AOC incl. makeup)

[Permanent link to this comic: https://xkcd.com/526/](https://xkcd.com/526/)
37 years of research... what do we have to show?
Quantified security is a weak hypothesis
Sciency & Business metrics
CVSS v3.0 - Base Score Metrics

Exploitability Metrics
- Attack Vector (AV)
  - Network (N)
  - Adjacent (A)
  - Local (L)
  - Physical (P)
- Attack Complexity (AC)
  - Low (L)
  - High (H)
- Privileges Required (PR)
  - None (N)
  - Low (L)
  - High (H)
- User Interaction (UI)
  - None (N)
  - Required (R)

Scope
- Scope (S)
  - Changed (C)
  - Unchanged (U)

Impact Metrics
- Confidentiality Impact (C)
  - High (H)
  - Low (L)
  - None (N)
- Integrity Impact (I)
  - High (H)
  - Low (L)
  - None (N)
- Availability Impact (A)
  - High (H)
  - Low (L)
  - None (N)
What's in your server?

Investing in cybersecurity with the Gordon-Loeb model

1. Invisible
2. Cost savings

US elections may spur cyber attacks
Target Breaches Another Data Breach Settlement
Morgan Stanley Suspected Russian Hackers
European Union lays down cybersecurity rules

Home Depot hackers expose emails

Customer card data hacked

Hacking scheme targets JPMorgan

Take your medicine

Gordon-Loeb model
The future
THE INTERNET OF THINGS
AN EXPLOSION OF CONNECTED POSSIBILITY

2020
50.1 BILLION
Fifteen popular经济学家 estimate there will be about 80 billion devices per hour or the planet.

2019
42.1 BILLION

2016
34.8 BILLION
Sensors that are already emerging will become more present—ranging from home appliances to connected desks, parking lot sensors, entertainment facilities and most utility meters are all starting to offer machine-to-machine communications.

2015
28.4 BILLION

2012
18.2 BILLION
According to Juniper Research, the global machine-to-machine communications will exceed 10 billion by 2015, twice the number of consumer electronic and intelligent building devices.

2011
11.2 BILLION

2012
8.7 BILLION
Just three years ago and the U.S. National Intelligence Council has recognized "Internet of Things" as one of the most "strategic" technologies with impacts that will last through 2025.

2014
14.4 BILLION
Today, there are twice as many objects connected to the Internet as there are people in the world.

2016
22.9 BILLION

2018
34.8 BILLION

2020
50.1 BILLION

1995
1,000,000
About one percent of the population of San Francisco.

2003
0.5 BILLION
As you increase connected devices in just 10 years.

2020
50.1 BILLION

INTERNET INCEPTION
2020
2003
1992

2018
34.8 BILLION

2016
22.9 BILLION

2012
18.2 BILLION

2011
11.2 BILLION

2010
42.1 BILLION

2019
28.4 BILLION

2015
28.4 BILLION

2012
11.2 BILLION

2003
0.5 BILLION

1992
1,000,000
Data
Predictive Models
Experimentation
Validation
Acknowledgements

IUSE: Collaborative Project: Engaged Student Learning: Design and Development, Level I: Broadening the Path to the STEM Profession through Cybersecurity Learning, #1700254
Images were taken from websites listed below:

- https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcTd8M0ih7NAQWBB1K9D7cyF68JcdnlGDKURI1MDACQ85KPbK4Of
cg
- https://res.cloudinary.com/dk-find-out/image/upload/q_80,w_1920,f_auto/A-Corbis-IH190312_l5pajc.jpg
- https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcQ0F7OZcMuAIQmUdZDxjrUMqi6iGs4XMLxge-Nhm3B7U11xclZTQ
- https://xkcd.com/526/
- https://ai2-s2-public.s3.amazonaws.com/figures/2017-08-08/8f8e0e4eca7cbc30cddea7f92d1dc0293342e9bb/3-Figure1-1.png
- https://www.suse.com/communities/blog/files/2017/01/cvss-v3-base-score-1024x532.png
- https://i.ytimg.com/vi/cd8dT0FuqQ4/maxresdefault.jpg
- http://www.digitalattackmap.com/
- http://www.geni.net/wp-content/uploads/2015/05/GENI-300x232.png
- http://3.bp.blogspot.com/-2fQIJGyzkRO/U366HOIXLGI/AAAAAAAAB8k/q0ZSfcIBQHw/s1600/kdd+logo.png
- https://image.freepik.com/free-photo/man-jumping-over-impossible-or-possible-over-cliff-on-sunset-background-business-concept-idea_1323-266.jpg
Open questions

- Do we need security metrics?
- What is the best approach to security metrics research?
- Why haven’t we still reached consensus of how security should be measured?
- Should there be standards like spec for security metrics?
- What is the future of security metrics?
- Validation: why is it so difficult? How should it be performed?