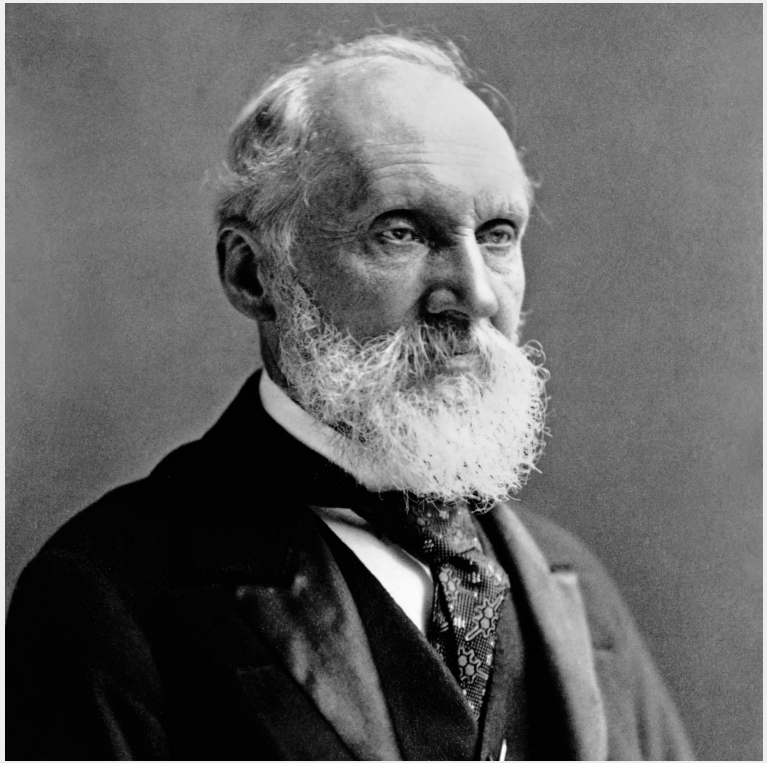

MISSION:
IMPOSSIBLE

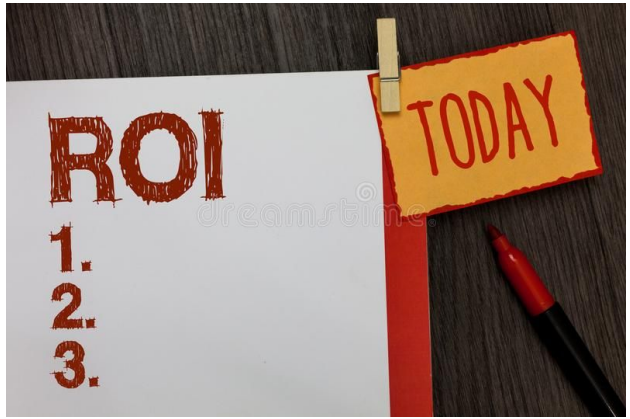
Why security metrics?

To measure is to know.
If you cannot measure it, you cannot improve it.

- Lord Kelvin




MEASURE
SUCCESS


ROI
1.
2.
3.
TODAY


RISK
1
2
3
4
5
6
7
8
9
10
11

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	LD
-30°C	K!
-40°C	SPIT GOES "CLINK"

THE KEY TO CONVERTING TO METRIC IS ESTABLISHING NEW REFERENCE POINTS. WHEN YOU HEAR "26°C," INSTEAD OF THINKING "THAT'S 79°F" YOU SHOULD THINK, "THAT'S WARMER THAN A HOUSE BUT COOL FOR SWIMMING." HERE ARE SOME HELPFUL TABLES OF REFERENCE POINTS:

LENGTH

1 cm	WIDTH OF MICROSD CARD
3 cm	LENGTH OF SD CARD
12 cm	CD DIAMETER
14 cm	
15 cm	BIC PEN
80 cm	DOORWAY WIDTH
1 m	LIGHTSABER BLADE
170 cm	SUMMER GLAU
200 cm	DARTH VADER
2.5 m	CEILING
5 m	CAR-LENGTH
16 m 4 cm	HUMAN TOWER OF *SERENITY* CREW

SPEED

kph	m/s	
5	1.5	WALKING
13	3.5	JOGGING
25	7	SPRINTING
35	10	FASTEST HUMAN
45	13	HOUSECAT
55	15	RABBIT
75	20	RAPTOR
100	25	SLOW HIGHWAY
110	30	INTERSTATE (65 MPH)
120	35	SPEED YOU ACTUALLY GO WHEN IT SAYS "65"
140	40	RAPTOR ON HOVERBOARD

VOLUME

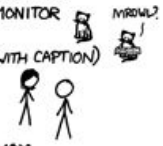
3 mL	BLOOD IN A FIELDMOUSE
5 mL	TEASPOON
30 mL	NASAL PASSAGES
40 mL	SHOT GLASS
350 mL	SODA CAN
500 mL	WATER BOTTLE
3 L	TWO-LITER BOTTLE
5 L	BLOOD IN HUMAN MALE
30 L	MILK CRATE
55 L	SUMMER GLAU
65 L	DENNIS KUCINICH
75 L	RON PAUL
200 L	FRIDGE

SO, WHEN IT'S BLOCKED, THE MUCUS IN YOUR NOSE COULD ABOUT FILL A SHOT GLASS.

RELATED: I'VE INVENTED THE WORST MIXED DRINK EVER.

MASS

3 g	PEANUT M&M
100 g	CELL PHONE
500 g	BOTTLED WATER
1 kg	ULTRAPORTABLE LAPTOP
2 kg	LIGHT-MEDIUM LAPTOP
3 kg	HEAVY LAPTOP
5 kg	LCD MONITOR
15 kg	CRT MONITOR
4 kg	CAT
4.1 kg	CAT (WITH CAPTION)
60 kg	LADY
70 kg	DUDE
150 kg	SHAQ
200 kg	YOUR MOM
220 kg	YOUR MOM (INCL. CHEAP JEWELRY)
223 kg	YOUR MOM (ALSO INCL. MAKEUP)



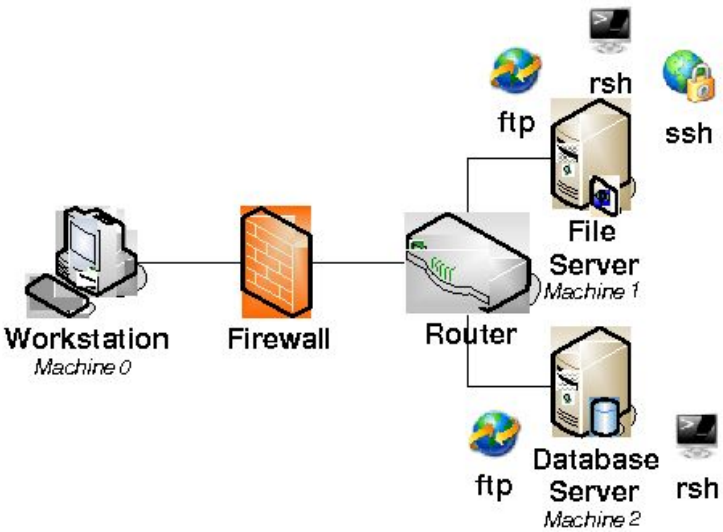
|< < PREV RANDOM NEXT > >|

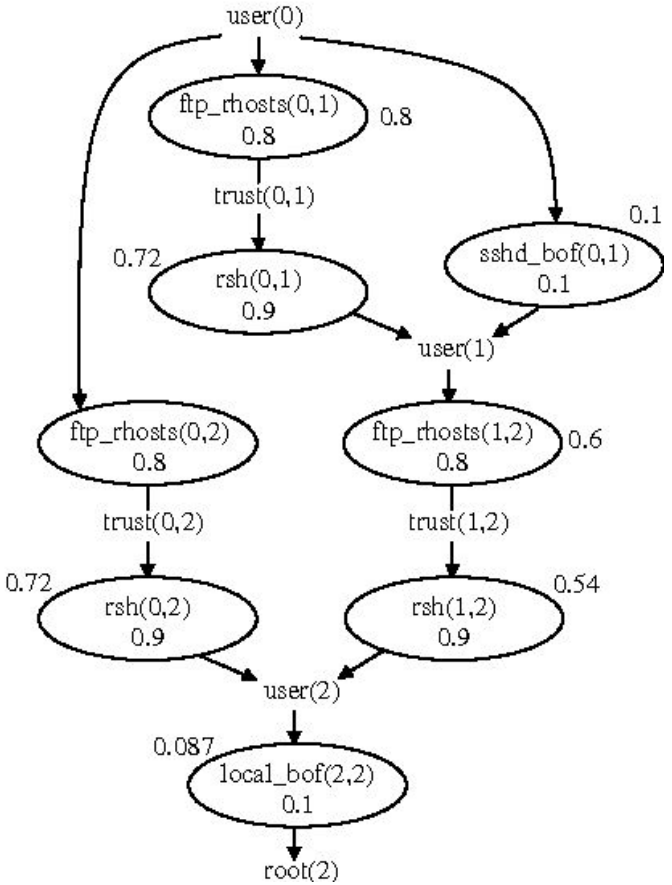
PERMANENT LINK TO THIS COMIC: HTTPS://XKCD.COM/526/

37 years of research… what do we have to show?

Quantified security is a weak hypothesis

Sciency & Business metrics


rsh
ftp
ssh
File
Server
Machine 1
Workstation
Machine 0
Firewall
Router
Database
Server
Machine 2
ftp
rsh


user(0)
ftp_rhosts(0,1)
0.8
0.8
trust(0,1)
0.1
0.72
rsh(0,1)
0.9
sshd_bof(0,1)
0.1
user(1)
ftp_rhosts(0,2)
0.8
ftp_rhosts(1,2)
0.8
0.6
trust(0,2)
trust(1,2)
0.72
rsh(0,2)
0.9
rsh(1,2)
0.9
0.54
user(2)
0.087
local_bof(2,2)
0.1
root(2)

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?

FEATURING SMITH SCHOOL PROFESSOR LARRY GORDON

INVESTING IN CYBERSECURITY WITH THE GORDON-LOEB MODEL

US elections may spur cyber attacks

Target Reaches Another Data Breach Settlement

Morgan Stanley Suspected Russian Hackers

CUSTOMER CARD DATA HACKED

European Union lays down cybersecurity rules

HOME DEPOT HACKERS EXPOSE EMAILS

Hacking Scheme Targets JPMorgan

GORDON-LOEB MODEL

1. INVISIBLE

2. COST SAVINGS

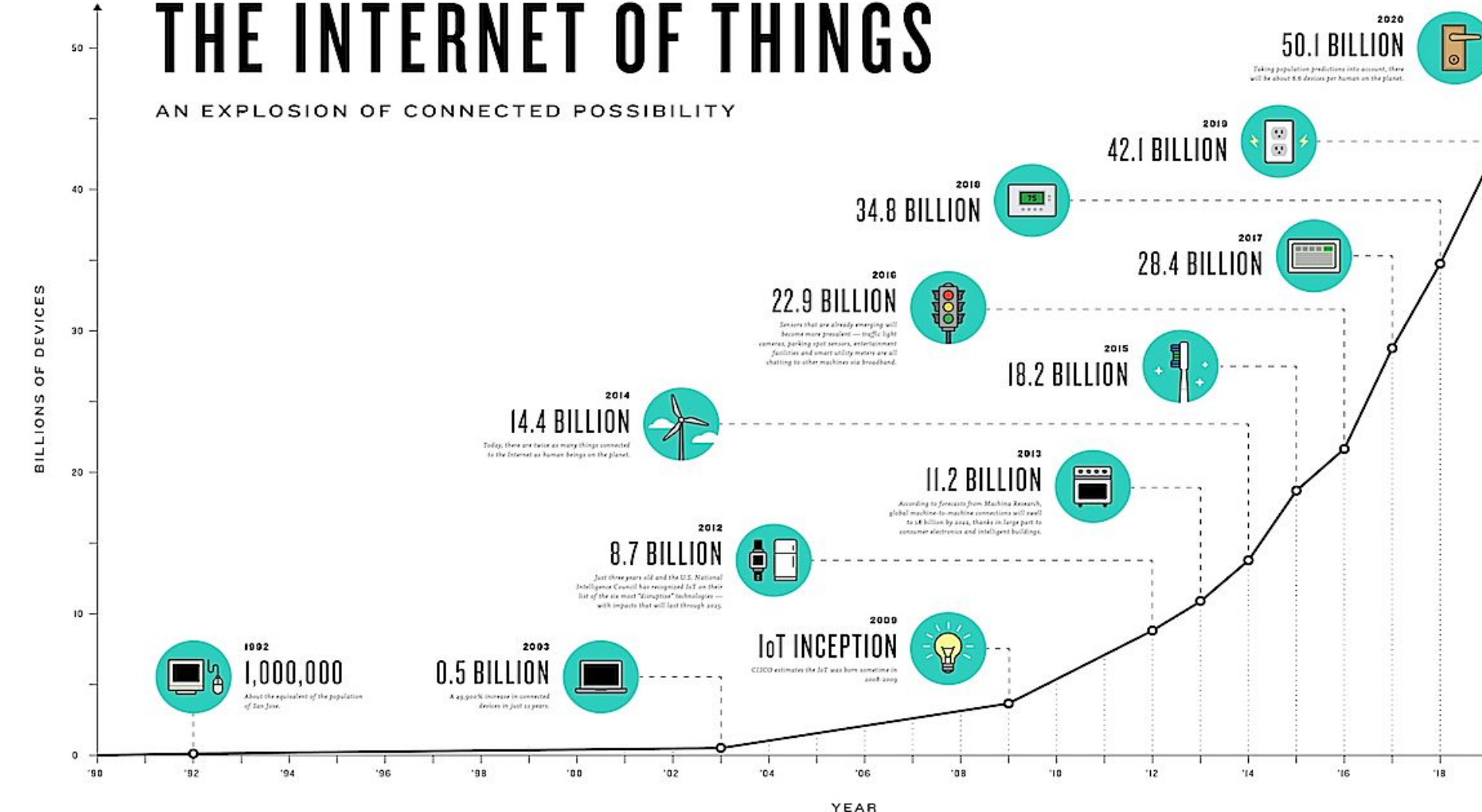
OUNT

TAKE YOUR MEDICINE

The future

THE INTERNET OF THINGS

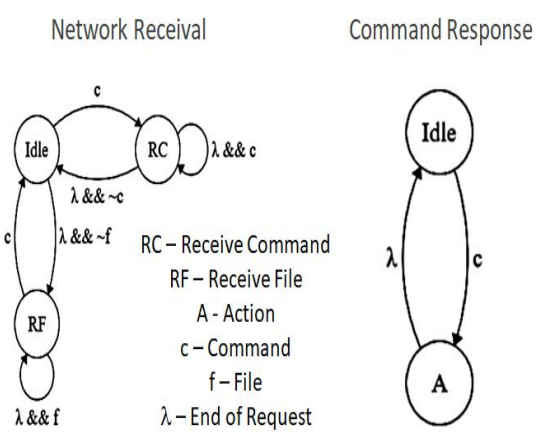
AN EXPLOSION OF CONNECTED POSSIBILITY



Digital Attack Map Top daily DDoS attacks worldwide

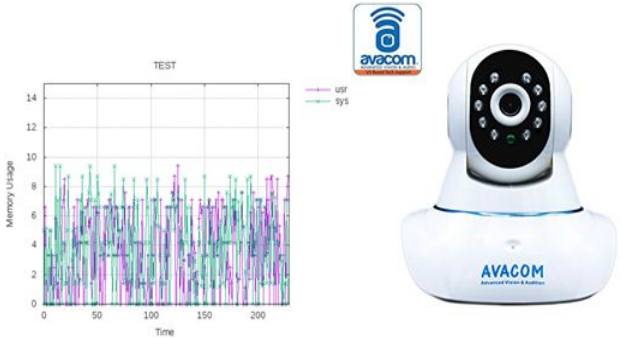
Map · Gallery · Understanding DDoS · FAQ · Al

KDD bringing together the data mining, data science and analytics community



Data
Predictive Models
Experimentation
Validation

geni
Exploring Networks of the Future




POSSIBLE
i m

Acknowledgements

IUSE: Collaborative Project: Engaged Student Learning: Design and Development, Level I: Broadening the Path to the STEM Profession through Cybersecurity Learning, #1700254

Disclaimer

Images were taken from websites listed below:

- https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcTd8M0ih7NAQWBB1K9D7cyF68JcdnlGDKURI1MDACQ85KPbK4Ofcg
- https://res.cloudinary.com/dk-find-out/image/upload/q_80,w_1920,f_auto/A-Corbis-IH190312_l5pagc.jpg
- https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcQ0F7OZcMuAlQmUdZDxjrUMgi6iGs4XMIxge-Nhm3B7U11xlclZTQ
- http://www.bitlanders.com/blogs/return-on-investment-roi-calculation-and-its-management/5528769
- 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.ncta.com/sites/default/files/2017-04/growth-of-internet-of-things-hero.jpg
- https://www.2-spyware.com/news/wp-content/uploads/news/omg-mirai-botnet-turns-iot-devices-into-proxy-servers_en.jpg
- http://www.digitalattackmap.com/
- http://www.geni.net/wp-content/uploads/2015/05/GENI-300x232.png
- http://3.bp.blogspot.com/-2fQIJGyzkR0/U366HOlXLGI/AAAAAAAAB8k/q0ZSfclBQHw/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?