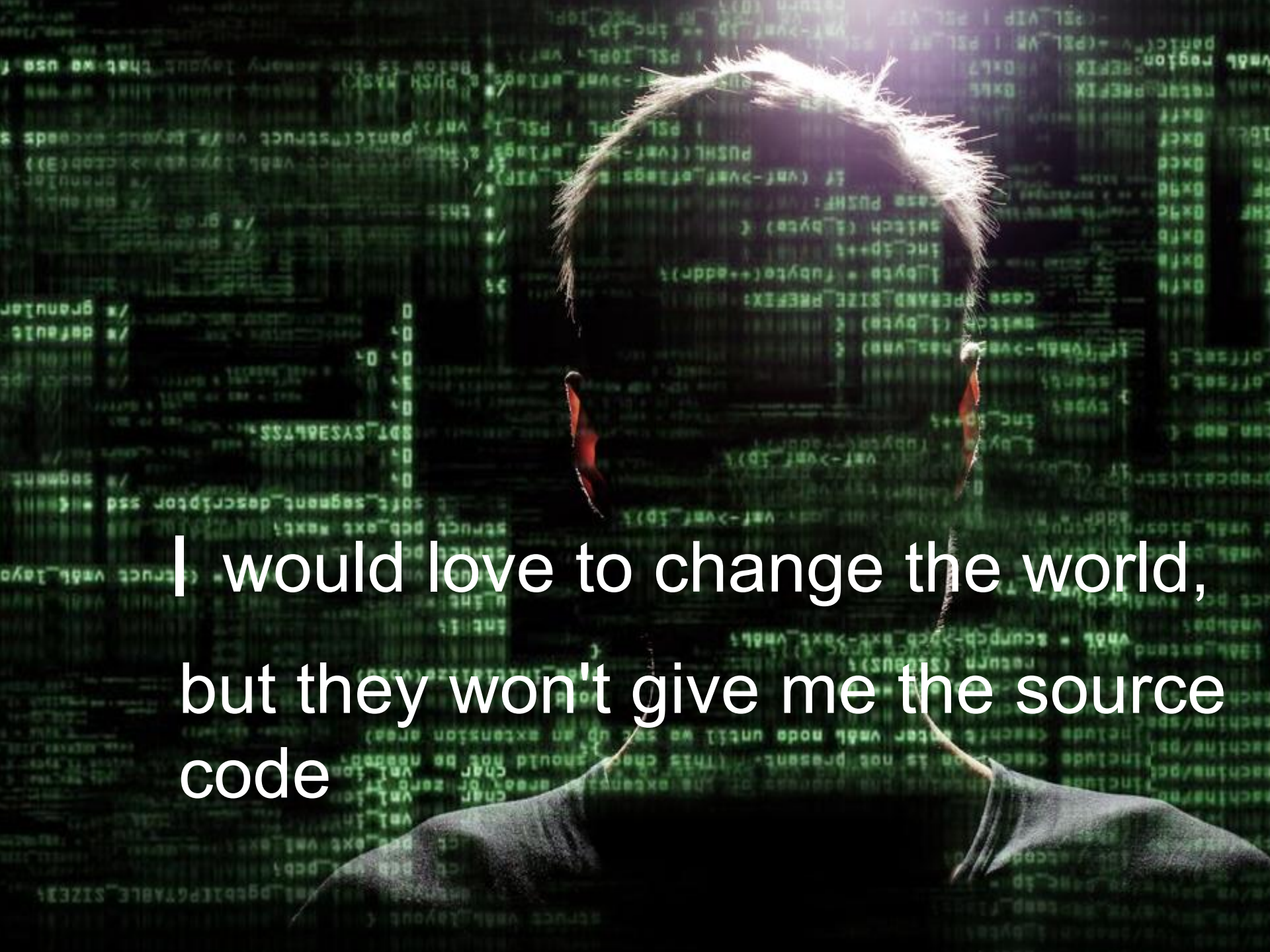
root64

Internet of Things – Challenges and Opportunities

Amit Dubey


I would love to change the world,
but they won't give me the source code

What is your digital DNA ?

webkay.robinlinus.com

privacy.net/analyzer

Social Media Exploits

browserspy.dk

What every Browser knows about you?

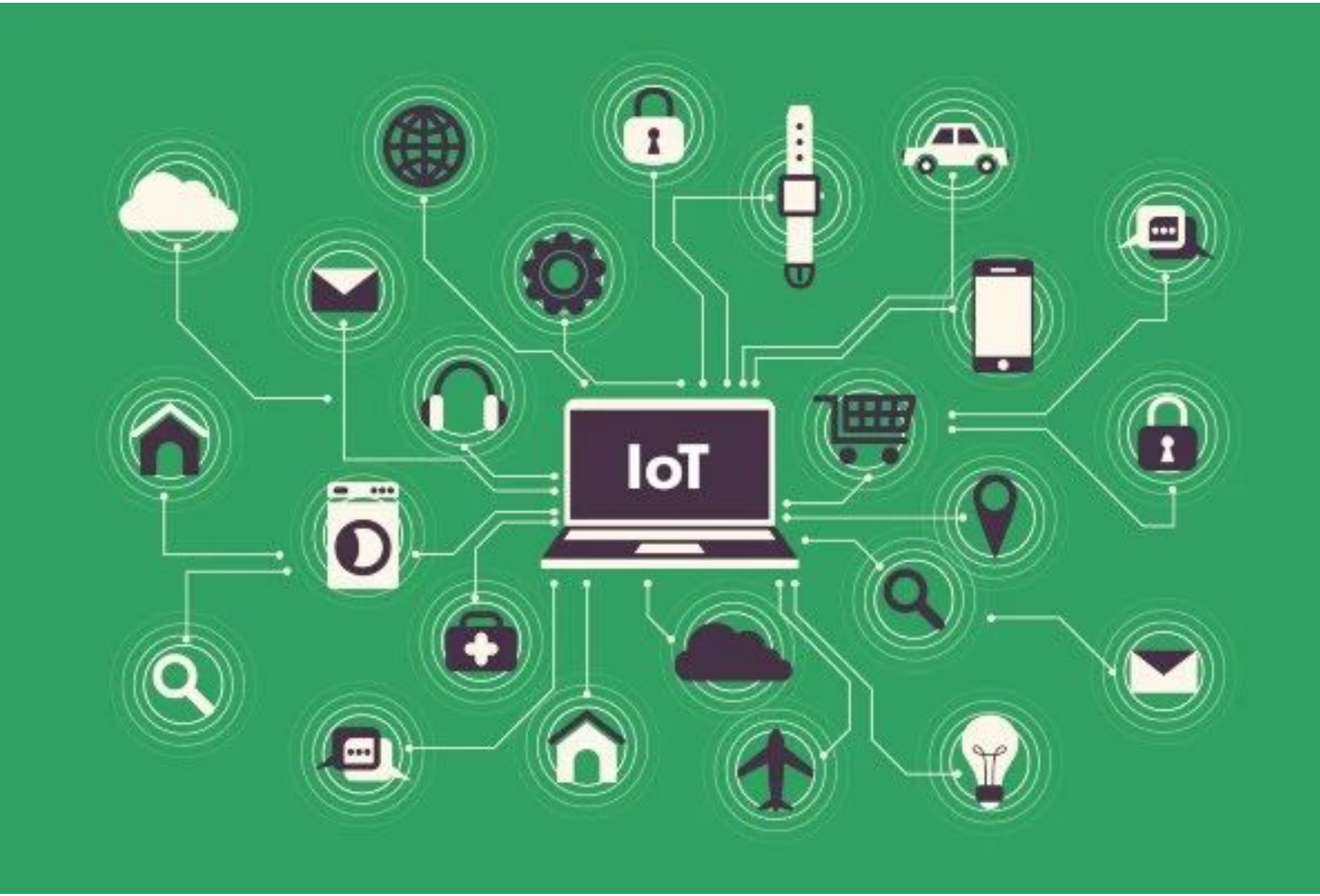
IOT Challenges in Future

Intelligent sensors with VR world

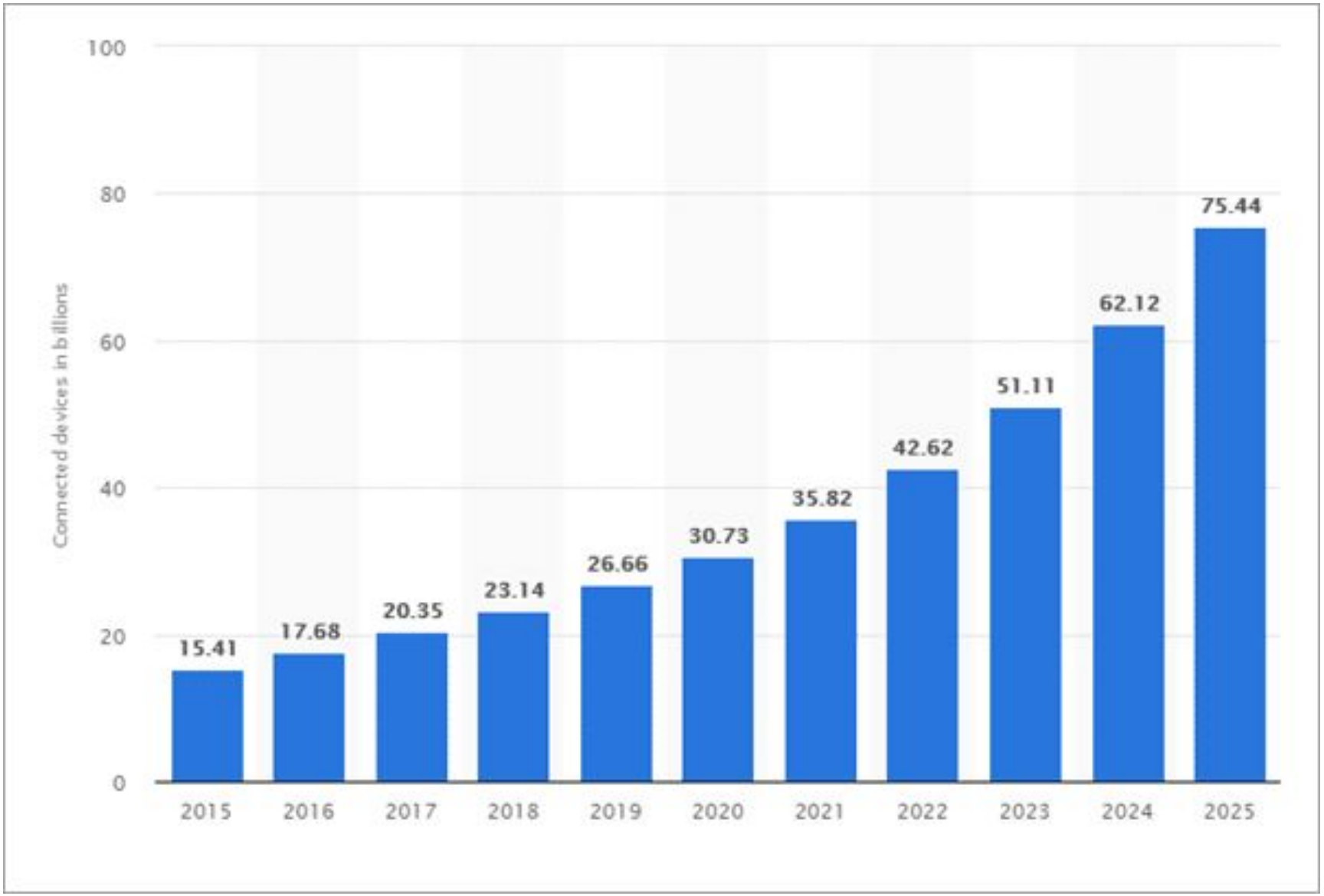
Quantum Computing

Meta verse

Artificial Intelligence


IoT

IOT Proliferation



IOT Devices - 2023

Increased Attack Surface

Google Home Voice Controller

Amazon Echo Plus Voice Controller

Amazon Dash Button

August Doorbell Cam

August Smart Lock

Kuri Mobile Robot

Belkin WeMo Smart Light

Footbot Air Quality Monitor

WeMo Insight Smart Plug

Philips Hue Bulbs and Lighting System

Top Cyber Attacks on IOT Devices

Verkada breach :

- In March-2021, Group of hackers succeeded to access and control 24000 of security cameras developed and managed by Verkada, a Silicon Valley-based company that sells security as a service.
- The group of hackers was able to get in by discovering a set of Verkada user credentials publicly exposed on the Internet. Once they breached the Verkada database, they moved laterally across the network and gained control over a super-admin account.
- From there, they were able to hijack control of the cameras to launch future attacks and access video footage stored on the cloud of Verkada's more than 24,000 client list.

The Mirai Botnet

- October - 2016, Largest DDoS attackever launched.
- The attack that targeted a DNS service provider Dyn, using a botnet of IoT devices.
- It managed to cripple Dyn servers and brought huge sections of the internet down. Media titans like Twitter, Reddit, CNN, and Netflix were affected.
- The botnet is named after the Mirai malware that it used to infect connected devices.
- Malware used the default name and password to login into the device, install itself, and repeat the process.

Top Cyber Attacks on IOT Devices

Cold in Finland

- November 2016, cybercriminals turned off the heating in two buildings in the Finnish cit

of Lappeenranta.

- After that, another DDoS assault was launched, forcing the heating controllers to reboo the system repeatedly, preventing the heating from ever turning on.
- This was a severe attack since Finland experiences severely low temperatures at that time of year.

Stuxnet

- Stuxnet is probably the most well-known IoT attack.
- Its target was a uranium enrichment plant in Natanz, Iran.
- During the attack, the Siemens Step7 software running on Windows was compromised, giving the worm access to the industrial program logic controllers. This allowed the worm's developers to control different machines at the industrial sites and get access to vital industrial information.

Top Cyber Attacks on IOT Devices

Cold in Finland

- November 2016, cybercriminals turned off the heating in two buildings in the Finnish cit

of Lappeenranta.

- After that, another DDoS assault was launched, forcing the heating controllers to reboo the system repeatedly, preventing the heating from ever turning on.
- This was a severe attack since Finland experiences severely low temperatures at that time of year.

Stuxnet

- Stuxnet is probably the most well-known IoT attack.
- Its target was a uranium enrichment plant in Natanz, Iran.
- During the attack, the Siemens Step7 software running on Windows was compromised, giving the worm access to the industrial program logic controllers. This allowed the worm's developers to control different machines at the industrial sites and get access to vital industrial information.

IOT Vulnerabilties

- Lack of visibility.
- Limited security integration.
- Open-source code vulnerabilities.
- Overwhelming data volume.
- Poor testing.
- Unpatched vulnerabilities.
- Vulnerable APIs.
- Weak passwords

AI Tools

ai.google/tools/

ai.facebook.com/tools/

aidemos.microsoft.com

lrpserver.hhi.fraunhofer.de

quickdraw.withgoogle.com

Attack Vectors

- SIM Cloning / eSIM
- Parallel Space/ WiFi Hack
- Data Privacy in my mobile phone.
- QR Code
- Whatsapp Hack
  - Call Forwarding
  - Voice mail
  - QR Code
  - Games
- Whatsapp Hack

Most Dangerous AI Crimes

- Audio and video impersonation,
- Driver less vehicles as weapons,
- Tailored phishing,
- Disrupting AI-controlled systems,
- Large-scale blackmail
- AI-authored fake news and Web Portals

Opportunities

- Logistics
- e-Commerce
- Healthcare
- NeuroScience
- Cyber Security
- Real Estate
- Retail Sector
- Airports
- Voice Powered Tech (ChatGPT)
- Metaverse
- Smart Cities
- Building & Home Security
- Smart Manufacturing
- Automotive
- Agriculture
- Wearables
- Energy

“Conversations are happening whether you are there or not”

Thanks