SAMSUNG

IT Академия
ИНТЕРНЕТ ВЕЩЕЙ

IoT[(1,2)] cybersecurity

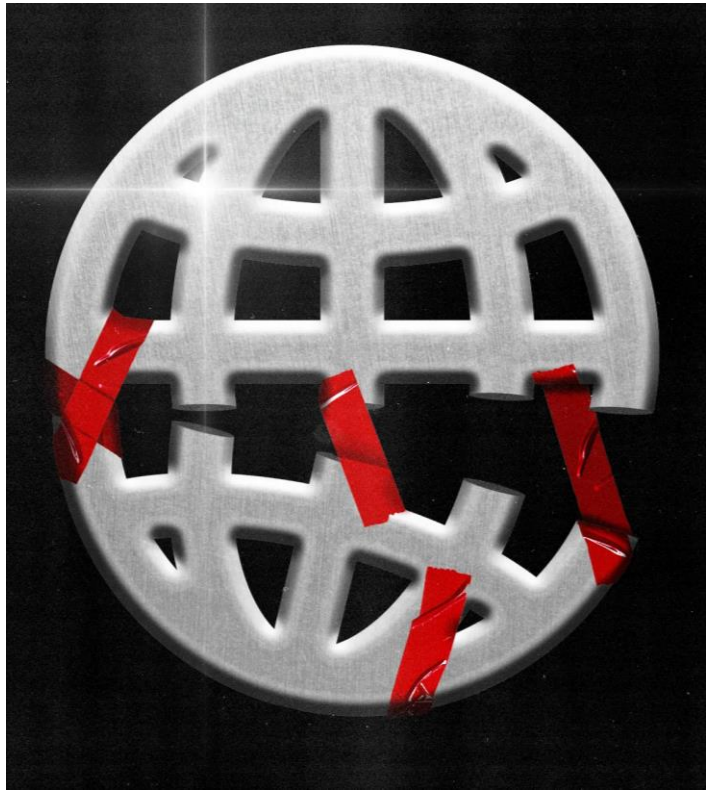
June 2021

Stanislav Polonsky

Samsung Advanced Institute of Technology - Russia

s.polonsky@samsung.com

(1) Internet of Threats
(2) S in IoT means Security



Why it’s important?

- 2022: 50 billion consumer IoT devices worldwide
- IoT’s insufficient attention to security, leading to:
- 30% IoT attacks growth year to year

Structure of the presentation

- Examples of IoT vulnerabilities: from toy to severe
- Advice on securing IoT

Mattel's spy-toy

- World's first "speaking doll" (2015)
- Uses WiFi to communicate with Google voice recognition server
- Vulnerabilities:
  - Mobile app
  - Cloud storage (partner company ToyTalk)

Security Flaws Open Connected Vacuum to Takeover

- Trifo's Ironpie M6 vacuum cleaner
- Checkmarx found high severity flaws
- Remote attacks on mobile app and comm protocol
  - Denial of Service
  - Embedded camera hacking
- Consumers should re-think buying smart home devices with potentially invasive cameras

Smart Doorbell: Many Brands Vulnerable to Attack

- Lead IoT introduction to homes
- Examples of vulnerabilities(1)
  - undocumented features
    - functional DNS service (malware delivery)
    - HTTP service w/ poorly protected credentials
  - mobile apps
    - HTTPS not enforced
    - root certificate via HTTP
  - hardware
    - no steal/tamper alarm (how about wi-fi jammer)
    - unprotected video on SD card
    - unprotected firmware w/ hardcoded credential

(1) Victure VD300 video doorbell

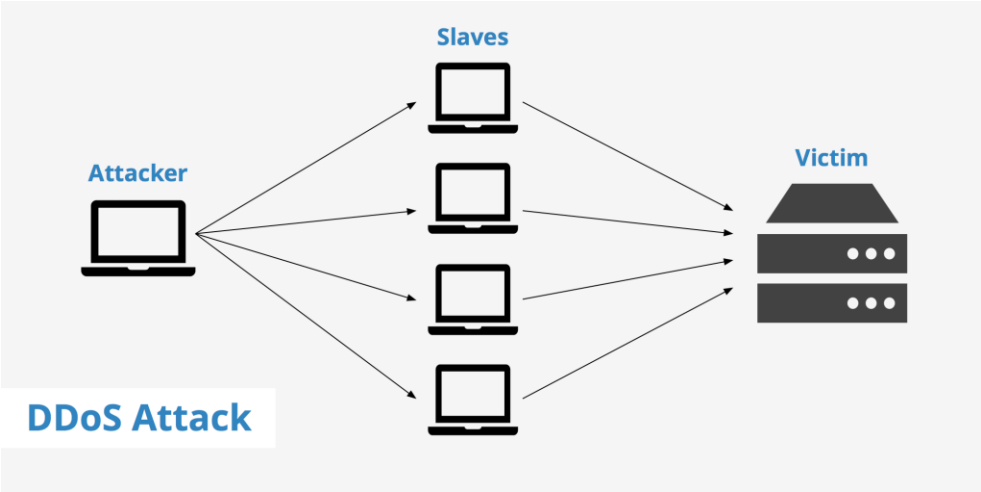
Your Philips Hue light bulbs can be hacked

- Virus:
  - jumps from bulb to bulb
  - changes light colour
- Vulnerability:
  - Zigbee communications protocol

Hackers are hijacking smart building access

- Linear eMerge E3 by Nortek Security & Control
  - corporates, factories, or industrial parks
- Applied Risk found numerous vulnerabilities
  - default credentials
  - privilege escalation
  - authorisation bypass
  - insecure storage of sensitive info
  - root access over SSH
- SonicWall : attackers actively target these devices as we see tens of thousands of hits every day, targeting over 100 countries

Weaponization of IoT: IoT botnets



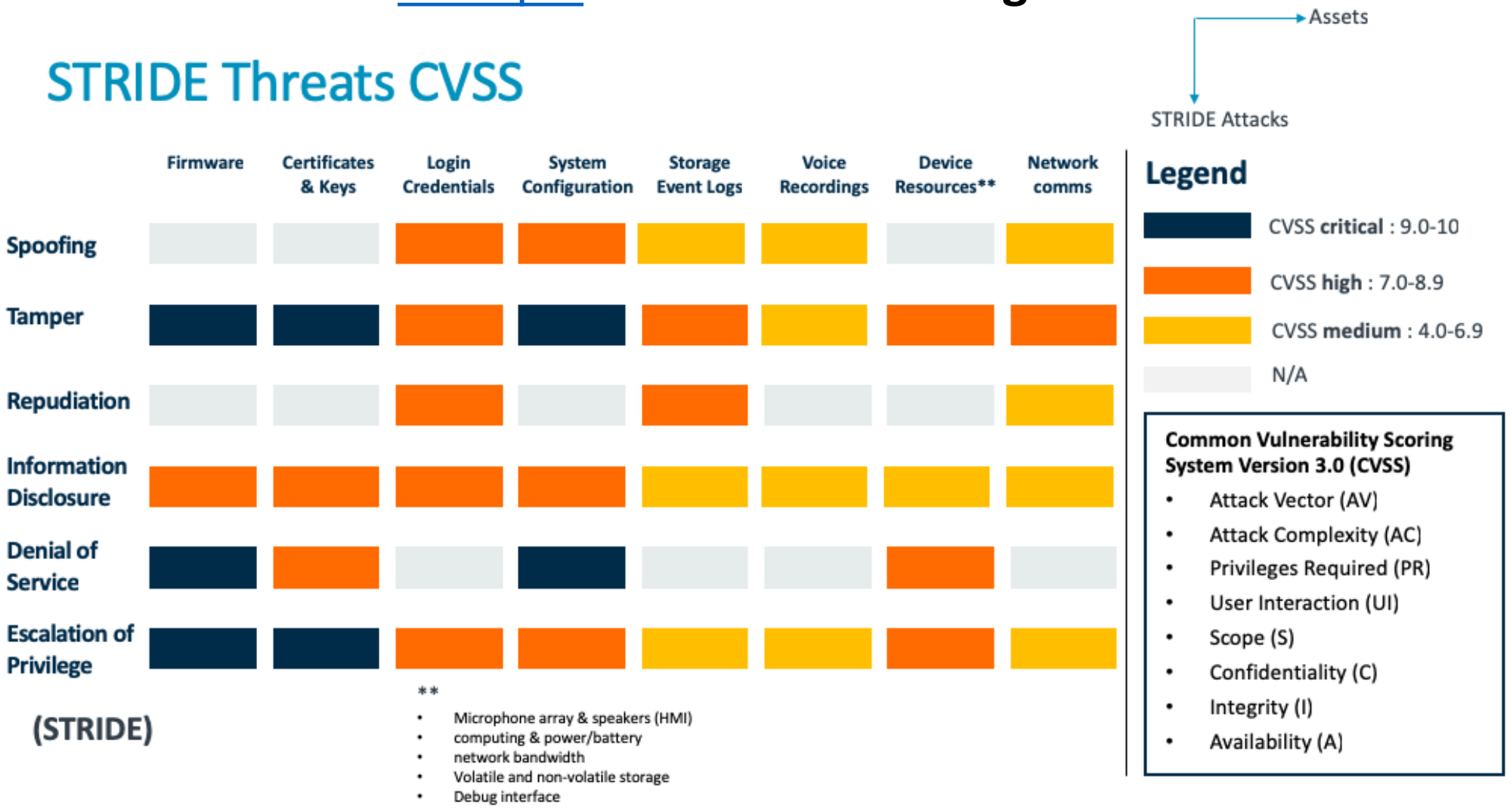
- Botnet:
  - many remotely controlled hacked computers
  - large-scale network attacks (e.g. DDoS)
- MalwareMustDie: Mirai botnet 2016
- Targets:
  - IP Cameras
  - Home routers
- Vulnerability
  - factory default credentials
- DDoS attacks
  - 1 Tbit/s
  - GitHub, Twitter, Reddit, Netflix, Airbnb

Advice 1: Understand Top IoT security vulnerabilities

- Weak, guessable default credentials
  - often publicly available
  - can be easily broken through brute-force attacks
- Unsecured network services
  - sensitive data can be compromised
  - authentication can be bypassed
- Inefficient update mechanisms
  - real-time security patches
  - firmware verification
- Improper data transfer and storage
  - lack of data encryption

Advice 2: Prioritize risks using structured approach

example of **Threat Modeling**



Next steps

- Media
  - Top IoT security vulnerabilities
  - Kaspersky Labs on IoT security: 1,2
- Coursera.org:
  - Introduction to Cyber Security Specialization
  - Cybersecurity and the Internet of Things
- Books
  - F.Chantzis , I.Stais , Practical IoT Hacking: The Definitive Guide to Attacking the IoT
  - D.Fagbemi , D.Wheeler The IoT Architect's Guide to Attainable Security and Privacy
- Project ideas
  - IoT «honeypot»
  - IoT vulnerability scanner
  - Smart Home Security