

Global Insights

IoT Security and Home Automation

- Dr. Ulrich Norbistrath
- IoT,
Home Automation,
Software Engineering,
Systems Integration
- Founder UINo.net

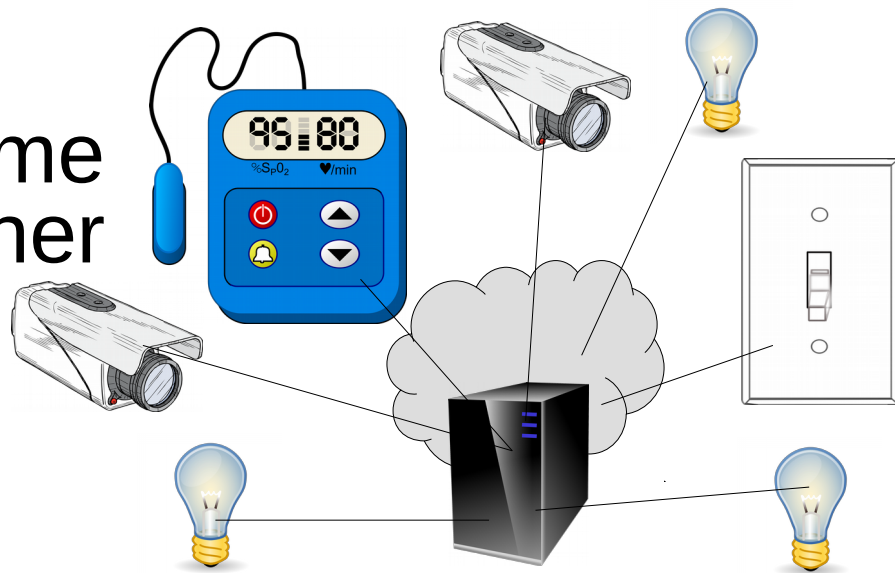


Security

- Software engineer's perspective
- Pay attention to IoT AND its security
- Don't make IoT an
IoBT (Internet of Broken Things)

Causes for Breakage

- Star topology/ no layered security
- Companies assume they can do updates for a fleet of devices
 - They can't
- Automation devices on same network as desktops or other infrastructure
- Default passwords

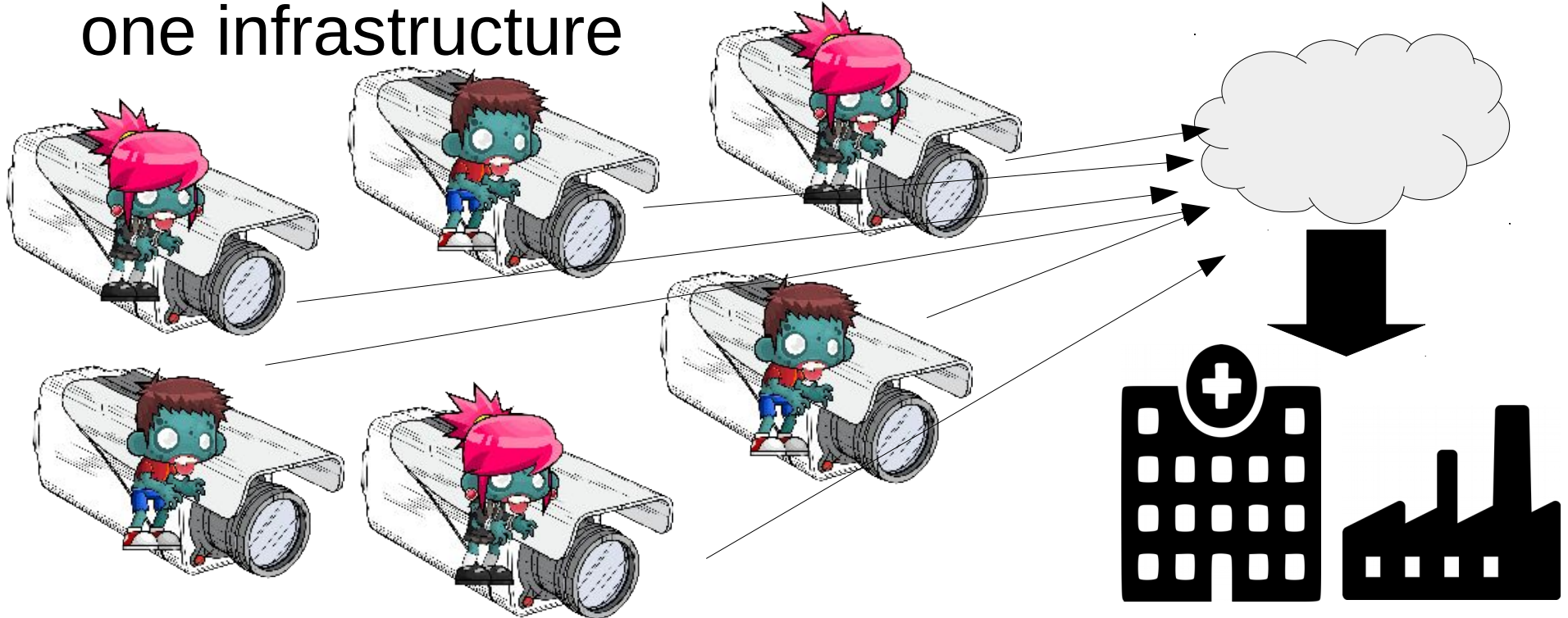


Example Break Downs

- Default passwords in devices and routers
 - Zombie webcams and routers
- WIFI networks very insecure - last widely deployed standard WPA 2 from before 2009 (IEEE 802.11w was specified 2009)
 - Deauth attack
 - Krack attack

Zombie Webcams

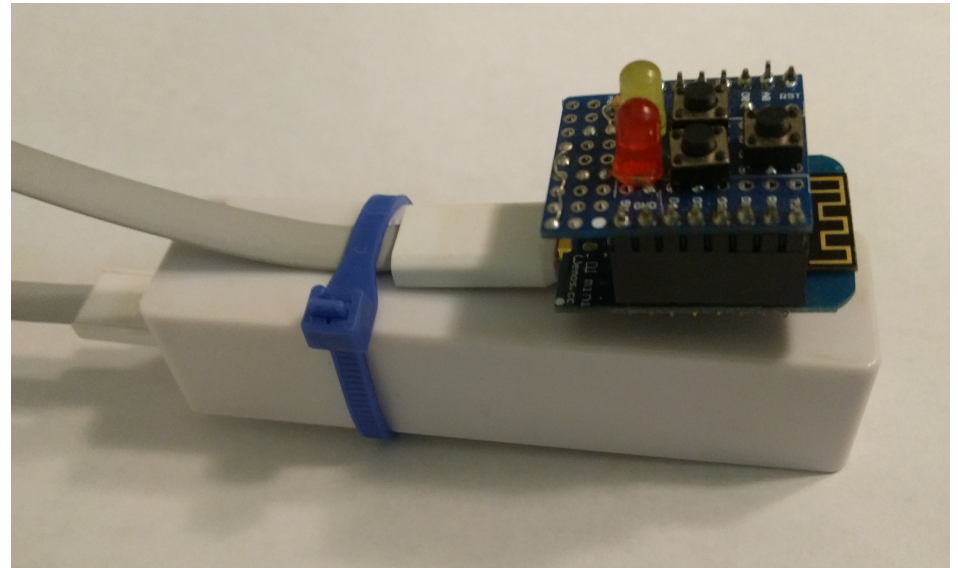
1 000 000 internet connected cameras attack
one infrastructure



- <https://www.law360.com/articles/861699/attack-of-the-zombie-webcams-ddos-attacks-and-the-insecure-iot>
- https://motherboard.vice.com/en_us/article/8q8dab/15-million-connected-cameras-ddos-botnet-brian-krebs

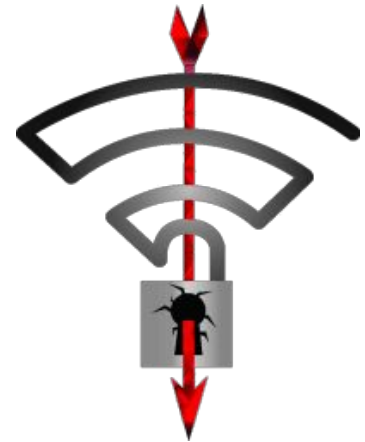
Deauth Attack

- Let me take down your internet for USD 2.50
- Countless denial of service attacks possible
 - Hospitals
 - Service institution
 - Factories
- If both router and client use IEEE 802.11w, not possible



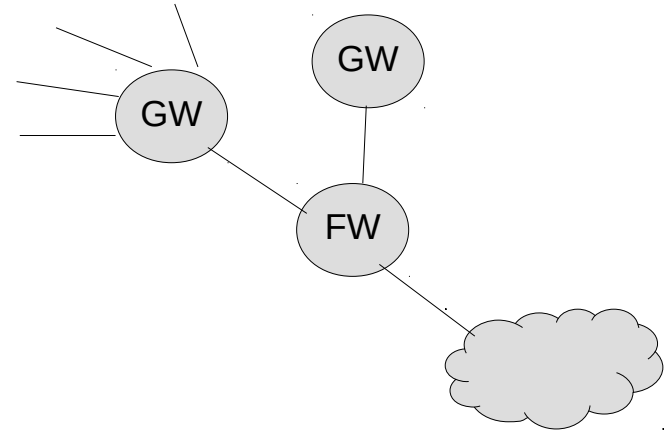
Krack Attack

- Most WIFI networks
 - All data of clients can be read
(basically all WIFI – even protected ones are like public WIFIs)
- Examples
 - Passwords for local devices are visible in clear text
 - Data filled in forms can be read
 - Patient data visible
 - Insurance and identity data visible



Counter Measures

- Layered architectures
- Avoid wireless
- Active and aware community
 - supporting and
 - auditing software and hardware
- Openness about core infrastructure
 - easy to audit
 - easy to update
- Build security into
 - life cycle management
 - maintenance



Let's prevent breaking the Internet of Things!