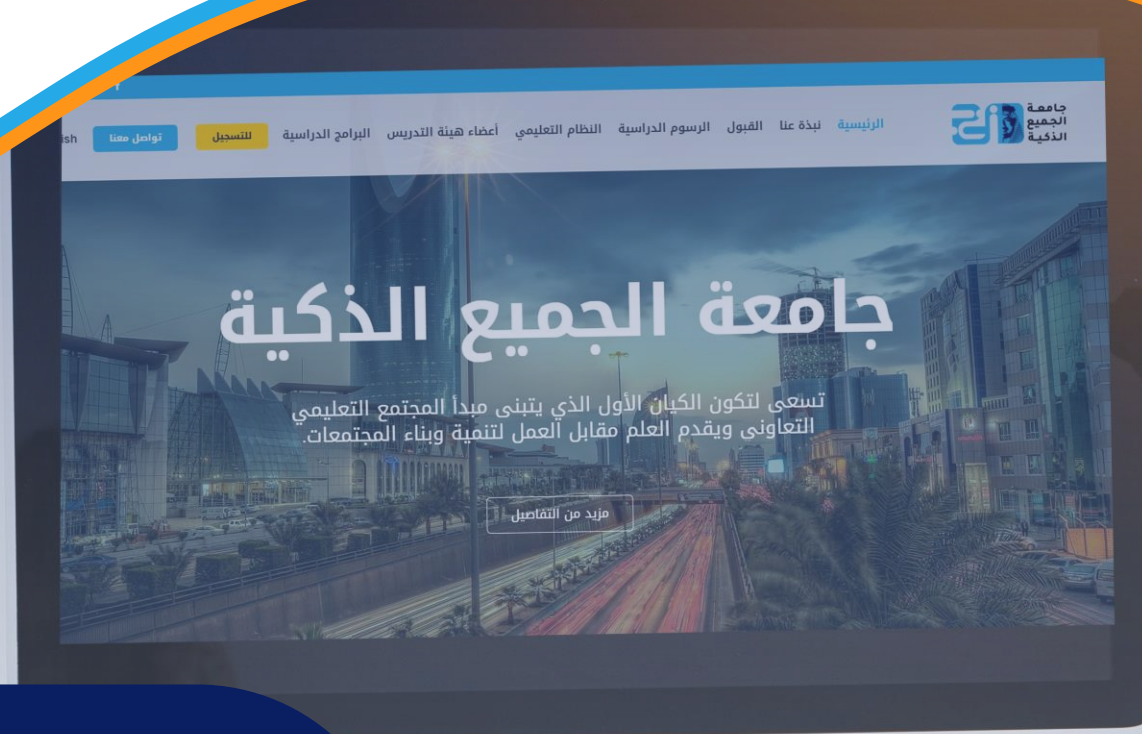




جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY



IoT Security
Prepared by Dr. Abdelrhman Ahmed
Lecture 4

IoT Attack History

**“ FOR EVERY LOCK, THERE IS SOMEONE OUT
THERE TRYING TO PICK IT OR BREAK IT ”**

~ DAVID BERNSTEIN

1. Water Utility SCADA “Supervisory control and data acquisition” System (Malicious Attack):

SCADA systems were penetrated as they were exposed to malicious actions where these hacks exploited weaknesses in the SCADA systems that remotely access the utility components. Generators, chlorine feeds, intake valves, and pump stations , all are essential to US water systems and cyber attacks could disrupt them all. The damage wouldn't only hinder water utility operations, it could have significant cascading effects both locally where the attack occurs and on a national level.

Date: 2011

Place: Illinois, USA.

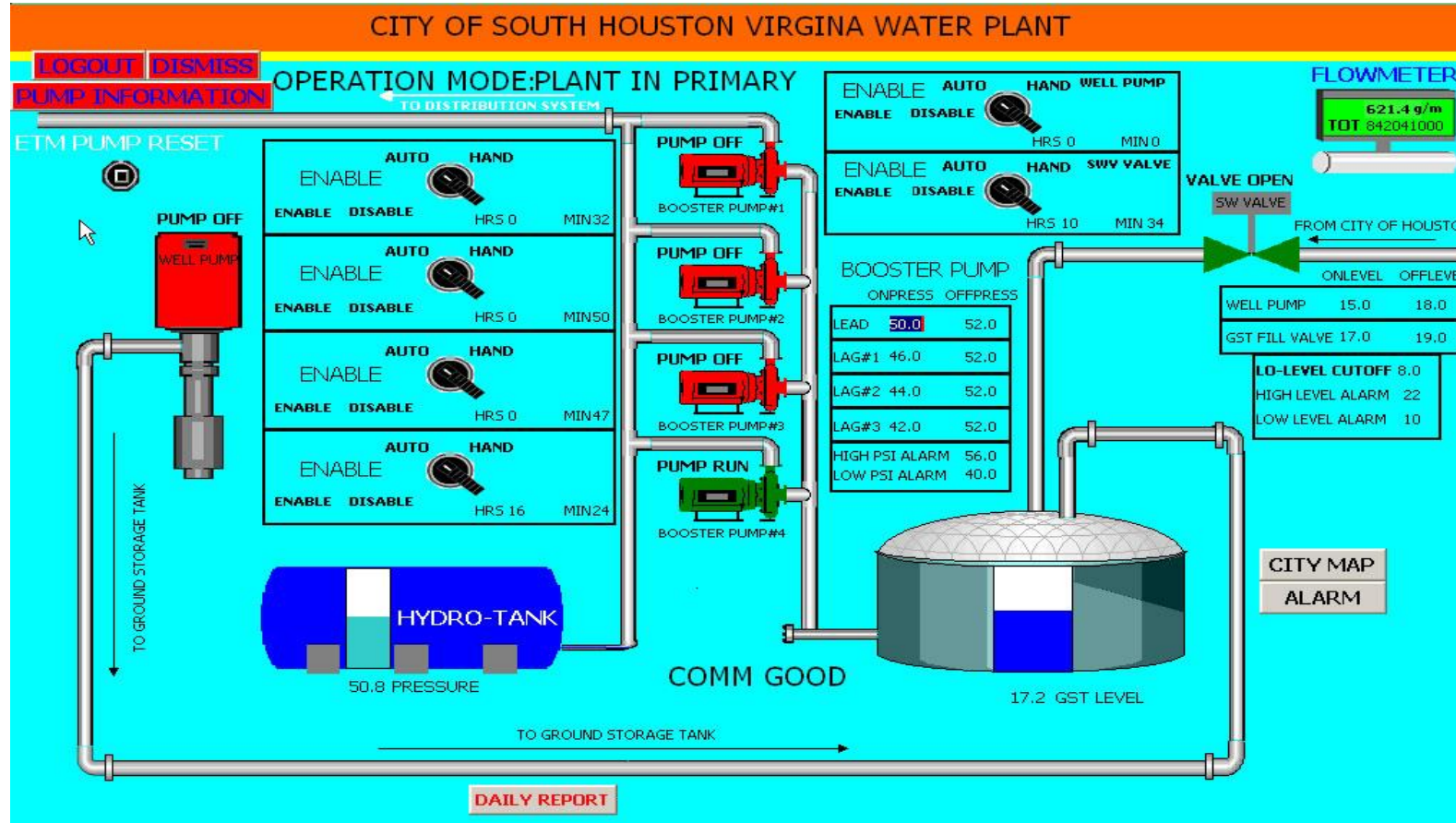
Loss: It is believed that the attackers breached the IT systems of the company that either manages or makes the SCADA system used at Curran-Gardner and stole customer usernames and passwords. The attackers then used this information to inflate the Curran-Gardner SCADA system.

Attack consequences: The ink wasn't dry on Joe's news when a twenty-something hacker using the name “pr0f” or “@pr0f_srs” published information of a successful penetration of the South Houston Water Utility. This attacker used an unrelated technique to gain access to the water utility and then posted several screenshots of the control system on PasteBin, including this one.



Chapter 04

EVOLUTION OF IOT ATTACKS



2. Puerto Rico smart meters (Data injection attack):

Smart meters are intended to improve efficiency, and reliability, and allow the electric utility to charge different rates for electricity at different times of the day. Puerto Rico electric utility – believed to be the Puerto Rican Electric Power Authority (PREPA) – Citing confidential sources, the FBI said it believes former employees of the meter manufacturer and employees of the utility were altering the meters in exchange for cash – from \$300 to \$1,000 for residential meters and about \$3,000 for commercial meters – and training others to do so.

Date: 2012

Place: Puerto Rico

Loss: The feds estimate that the Puerto Rican utility's losses from the smart meter fraud could reach \$400 million annually.

Attack consequences: The FBI believes those responsible hacked into the smart meters using an optical converter device – such as an infrared light – connected to a laptop that allows the smart meter to communicate with the computer. After making that connection, the settings for recording power consumption were changed using software that can be downloaded from the internet. Strong magnets were placed on the devices to slow the meters were also believed to be used, particularly at night, in some cases.



3. Bashlite Botnet (Malicious Attack):

L3 has been working with security firm Flashpoint to observe the growth of the botnet, which the malware uses to carry out its attack. Threatpost reported that in July, the researchers tracked command-and-control (C&C) locations that were linked to the malware and found that they were communicating with only 74 bots. At a later time, the researchers observed the C&C servers communicating with about 120,000 bots.

Date: 2014

Place: Brazil, Taiwan and Colombia.

Loss: A large percentage of the 1 million infected devices were located in Taiwan, Brazil, and Colombia, L3 reported. It seems many of these bots were using generic, white-labeled DVRs where they were abused with DDoS attacks.

Attack consequences: According to researchers, 95 percent of the infected devices are digital video recorders (DVRs) and cameras, four percent are routers, and the rest are Linux servers.

DVRs are known to contain numerous serious vulnerabilities, including hardcoded passwords, that make them a tempting target for cybercriminals. In some cases, devices from multiple vendors share vulnerable code, providing attackers and even with a larger victim base.



4. University of Michigan Traffic Light (WIFI Attack):

According to the researchers, MIT continues, there were three major problems with the traffic lights: they operate over a wireless network that's unencrypted; they share common user names and passwords; and their debugging ports aren't especially challenging to mount an attack on. The researchers point out to MIT that this "systemic lack of security consciousness" leaves the shared traffic light systems in nearly all U.S. states exceptionally vulnerable should someone with a bit of computer savvy decide to mess with them.

Date: 2014

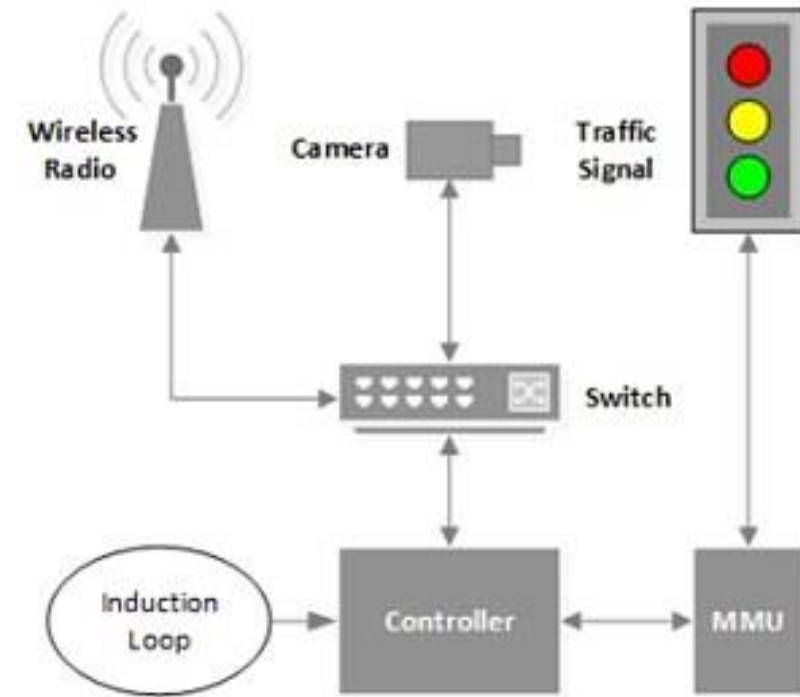
Place: USA.

Loss: Nearly one million researchers partnered with a local Michigan road agency to hack into almost 100 wirelessly networked traffic lights.

Attack consequences: More than 40 states currently use such systems to keep traffic flowing as efficiently as possible, helping to reduce emissions and delays. The team, led by University of Michigan computer scientist J. Alex Halderman, found three major weaknesses in the traffic light system: unencrypted wireless connections, the use of default usernames and passwords that could be found online, and a debugging port that is easy to attack.

4. University of Michigan Traffic Light (WIFI Attack):

There are sensors that detect cars, controllers that use the sensor data to control the lights at a given intersection, radios for wireless communication among intersections, and malfunction management units (MMUs), which return lights to safe fallback configurations if an 'invalid' configuration occurs. For example, if somehow every light at an intersection is green, the system might fall back to having them all become flashing red lights.



5. BMW connected drive system (Man-In-The-Middle Attack):

Cars with built-in modems are sending data to their manufacturers - German motorist's club ADAC wanted to know what exactly gets sent. c't connected ADAC with a specialist who analyzed the data transmissions, using the example of BMW's ConnectedDrive technology. He discovered security vulnerabilities that even allow unauthorized attackers to open the vehicles.

Date: 2015.

Place: USA.

Loss: Nearly one allowed researchers to imitate BMW servers and send remote unlocking instructions to vehicles.

Attack consequences: The attack took advantage of a feature that allows drivers who have been locked out of their vehicles to request remote unlocking of their cars from a BMW assistance line.

6. Ukrainian power grid (Intrusion Attack):

The attack on the power station occurred in the afternoon. An employee was working at his desk organizing papers when he noticed something very odd. As if by magic, the cursor on his computer began to move around the screen on its own. The worker watched – mouth likely agape – as the cursor moved towards buttons that control a substation's circuit breakers, clicking on a box to open them – taking the substation offline, leaving 225,000 residents in the dark. The employee made every effort to regain control of the computer. But it was too late. The attackers had already logged him out.

Date: 2015.

Place: The Ukrainian Kyivoblenergo, a regional electricity distribution company.

Loss: Anywhere from 200,000-230,000 Ukrainian citizens.

Attack consequences: The company's computer and SCADA systems were attacked, disconnecting 30 substations for three hours. As many as 230,000 customers lost power – approximately half of the homes in the Ivano-Frankivsk region in Ukraine (population about 1.4 million). The tool used was malware known as **BlackEnergy**.

6. Ukrainian power grid (Intrusion Attack):

The company's computer and SCADA systems were attacked, disconnecting 30 substations for three hours. As many as 230,000 customers lost power – approximately half of the homes in the Ivano-Frankivsk region in Ukraine (population about 1.4 million). The tool used was malware known as BlackEnergy.



7. Tesla Model S Remote Hack (Intrusion Attack):

The attack on the power station occurred in the afternoon. An employee was working at his desk organizing papers when he noticed something very odd. As if by magic, the cursor on his computer began to move around the screen on its own. The worker watched – mouth likely agape – as the cursor moved towards buttons that control a substation's circuit breakers, clicking on a box to open them – taking the substation offline, leaving 225,000 residents in the dark. The employee made every effort to regain control of the computer. But it was too late. The attackers had already logged him out.

Date: 2016.

Place: Keen Security Lab of Tencent, a Chinese Technology conglomerate

Loss: We have verified the attack vector on multiple varieties of Tesla Model S. It is reasonable to assume that other Tesla models are affected.

Attack consequences: a remote attack that compromises CAN Bus to achieve remote controls on Tesla cars.

Tesla Incident

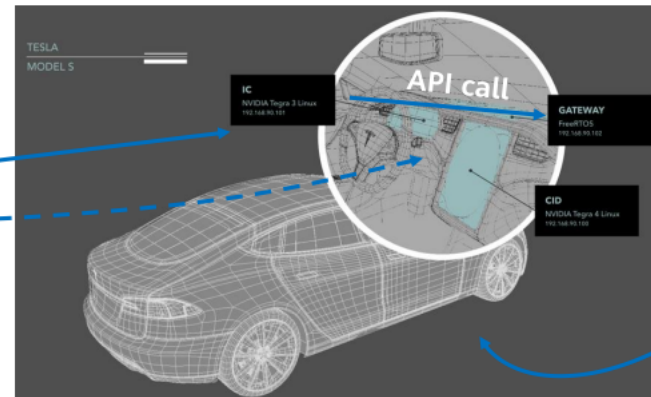
- The in-vehicle system is intruded, causing a vehicle to be remotely started or stopped.

- ② Forge a connection to communicate with the background and obtain the password for the in-vehicle system.



- ③ Log in to the system and deliver commands to the CAN bus through the gateway.

- ① Analyze the hardware and find the removable storage card that contains the background remote communication certificate and password stored in plaintext.



Attacks can cut off power during the driving process.

- ④ Deliver commands to the CAN bus to control the vehicle's behavior, including vehicle startup and shutdown, as well as door opening and closing.

- No protection measures are taken for local key information causes this incident.

8. MIRAI botnet (Malware Attack):

An IoT botnet (a network of computers, each of which runs bots) was used to execute the worst DDoS attack against Internet performance management services provider Dyn back in October 2016. As a result, several websites went offline, including majors like CNN, Netflix, and Twitter.

Date: 2016.

Place: USA.

Loss: After becoming infected with Mirai malware, computers continuously search the web for susceptible IoT devices before infecting them with malware by logging in using well-known default usernames and passwords. These gadgets included digital cameras and DVR players, for example.

Attack consequences: telecom company OVH was hit by a distributed denial-of-service (DDoS) attack. Experts were struck by how the assault was 100 times larger than similar threats. The following month, over 175,000 websites suffered, as Dyn, a managed DNS (Domain Name System) provider, was hit by another powerful DDoS attack. Much of the eastern United States and some of Europe suffered a significant drop in Internet quality.

DDoS Attack on Network Cameras in the U.S.

- The large-scale DDoS (Distributed Denial of Service) attack was launched by botnets composed of IoT devices that were infected with Mirai malware.
- "Zombies" refer to network cameras, digital video recorders and intelligent routers.
- Mirai botnets infected millions of devices, and only one tenth of them were involved in this DDoS attack.



From 11:00 to 17:00 (UTC time) on October 21, 2016, Internet services were unavailable in several cities in the U.S., and **nearly half of the network was disconnected.**

9. CCTV botnet (DDoS Attack):

Reports show that , there were 245 million surveillance cameras operating around the world. And this only accounts for the professionally installed ones. There are likely millions more that were installed by unqualified professionals, with even fewer security precautions.

Date: 2016.

Place: France.

Loss: Around 150,000 hacked CCTV cameras were used as part of a botnet to attack the infrastructure of a French web hosting company.

Attack consequences: Further investigation of the offending IPs showed that they belonged to CCTV cameras, all accessible via their default login credentials. And that's not all. Looking through the camera lens we also spotted a familiar sight—a storefront in a mall located not five minutes away from our offices!

10. Amnesia Botnet (Botnet Attack):

The threat, believed to be a variant of the Tsunami botnet, has been analyzed in detail by researchers at Palo Alto Networks. The botnet targets embedded systems, particularly DVRs made by China-based TVT Digital, which are sold under more than 70 brands worldwide.

Date: 2017.

Place: Produced by China-based firm, TVT Digital Technology Co., Ltd..

Loss: The security hole likely remains unpatched and an Internet scan conducted by Palo Alto Networks shows that there are roughly 227,000 vulnerable DVRs in the United States, Taiwan, India, Israel, Turkey, Malaysia and many other countries. A different search carried out via the Censys.io project revealed more than 700,000 IP addresses.

Attack consequences: it has virtual machine (VM) evasion capabilities – experts say this is the first Linux malware that attempts to evade sandboxes.

11. Saudi petrol chemical plant triton attack (Malware Attack):

In January 2017, computers went dark at the National Industrialization Company, Tasnee for short, which is one of the few privately owned Saudi petrochemical companies. Computers also crashed 15 miles away at Sadara Chemical Company, a joint venture between the oil and chemical giants Saudi Aramco and Dow Chemical. Within minutes of the attack at Tasnee, the hard drives inside the company's computers were destroyed and their data wiped clean, replaced with an image of Alan Kurdi, the small Syrian child who drowned off the coast of Turkey during his family's attempt to flee that country's civil war.

Date: 2018.

Place: Saudi Arabia

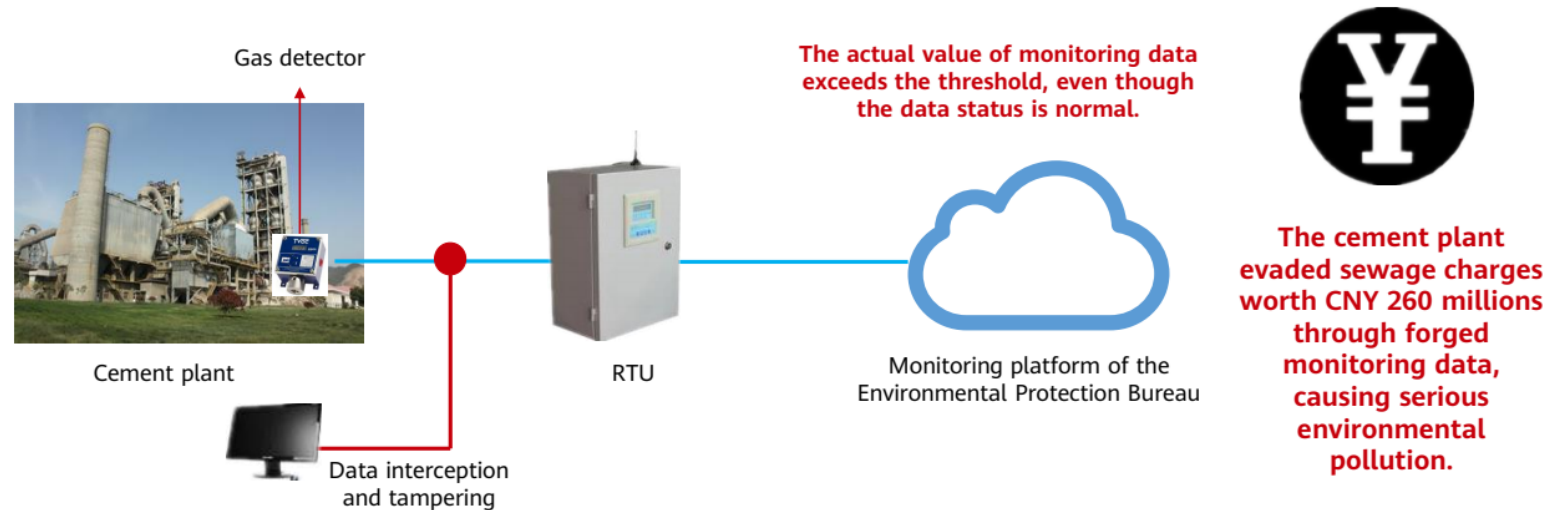
Loss: The malware was specifically targeting the safety override systems, in an overt attempt to cause catastrophic damage

Attack consequences: The malware appears to be designed to force a malfunction in the 'Triconex' Safety Instrumented System (SIS), a popular logic controller made by Schneider Electric, Cyberscoop reported. The SIS is used to control industrial equipment, and it is believed that the malware was intended to cause machinery to operate outside of normal parameters until it suffered serious damage.



Nanjing Environmental Protection Bureau Incident

- The local network was intruded, and environmental monitoring data was tampered with.



- Encryption and integrity protection are not carried out during data transmission, which allows the violation to be possible.

12. Stuxnet Worm (Malware attack) :

Stuxnet is a computer worm that was originally aimed at Iran's nuclear facilities. The original Stuxnet malware attack targeted the programmable logic controllers (PLCs) used to automate machine processes used to turn uranium into nuclear fuel. NSA & ISRAELI military wrote a program that digitally mapped out the workings of Iran's Natanz plant where they ordered a cyber attack to slow down Iran's nuclear program.

Date: 2010

Place: Iran

Loss: The Stuxnet worm spun many of the centrifuges out of control, blowing them up, all without the Iranian figuring out what was causing the explosions. It took out nearly 1000 centrifuges about one-fifth of those operating.

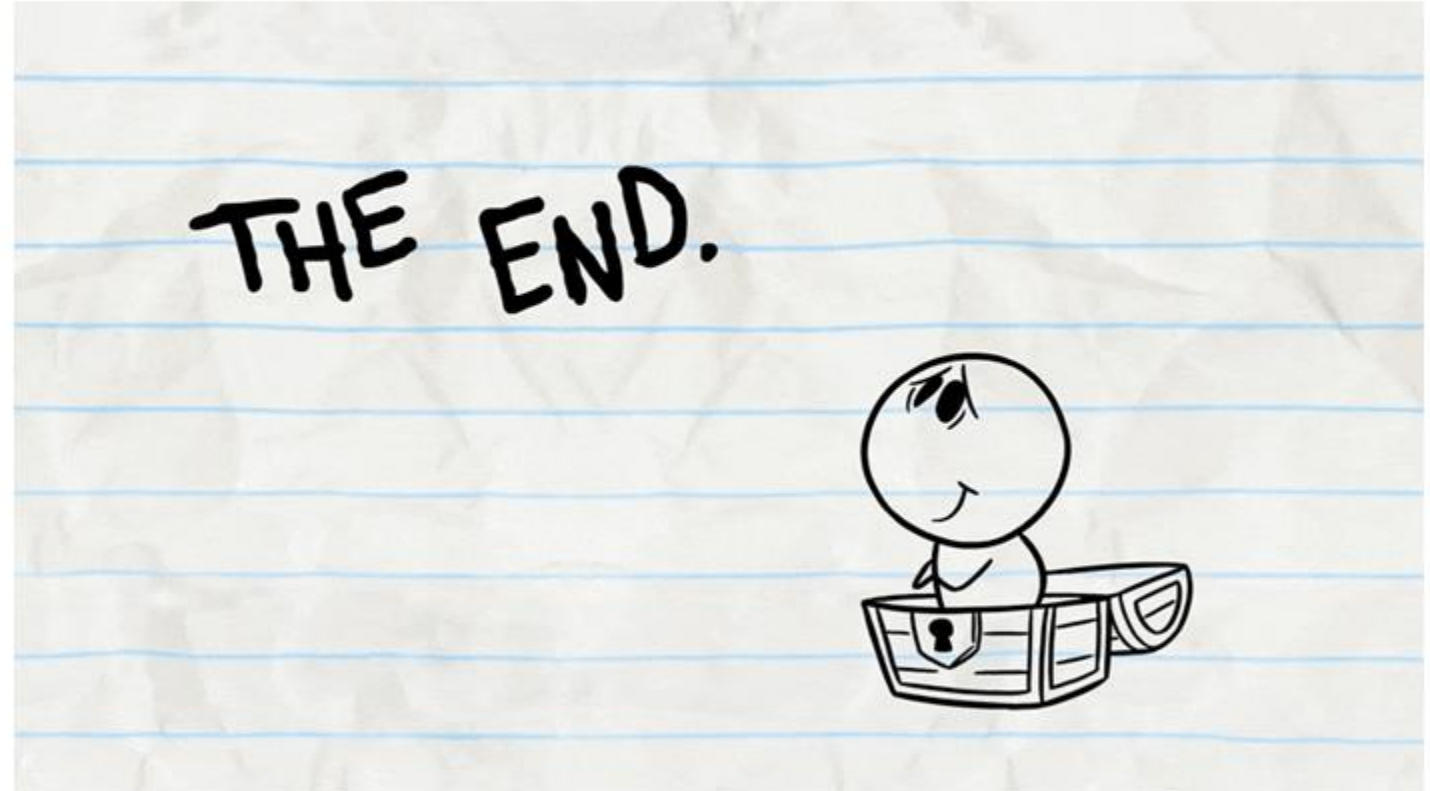
Attack consequences: the worm takes over control of centrifuges causing them to spin too fast or too slow, they become unbalanced and in some cases explode. The attackers even secretly recorded what a normal day at the plant looked like & then played those readings back to plant operators so they didn't think anything was wrong as the centrifuges were tearing themselves apart. The US believes the attack set back Iran's nuclear program by up to 2 years.



The End

Please feel free to contact me anytime if you have any questions

Abdelrhman Ahmed Refaat:
abdelrhmanahmedrefaat@gmail.com



جامعة القادسية
EVERYONE'S SMART UNIVERSITY