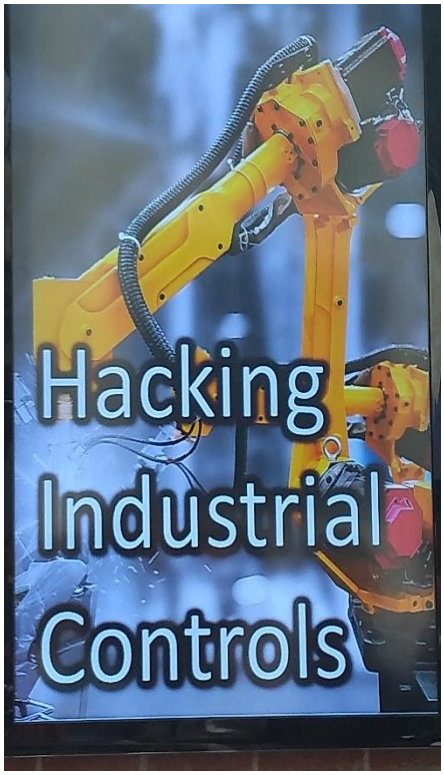
IOT and Hacking of Industry Controls

In June there was an Information Security Forum held at Olympia in London, it was a 3 day event where all security vendors, & penetration testers attended and shared the latest breaches and vulnerabilities. They even shared how they breached various systems to prevent crippling attacks. This year was the year of I.O.T "Internet of Things" and engineering equipment risk.

IoT is defined as everyday objects with computing devices embedded in them that have a means to send and receive data over the internet.

I.E :- Amazon Echo, google home voice controller, ring door bell, smart lighting, smart watch, smart locks, Teslar car, Nest smart home.

IoT devices have many applications that are designed to make life easier and simpler. Think of engineers being able to access a device, perform remote diagnosis and remediating any issue.



How !.....

IOT devices and industry devices lack general security, and have security vulnerabilities.

- Weak, Guessable, or Hardcoded
- Use of Insecure or Outdated Components
- Lack of Device Management
- Connected to 3rd party main networks which are secure until the device is connected allowing a gateway onto the main network, known as network hoping.
- Lack of a secure frequent system updates being applied

What could happen !....

In the top photo "pen test partners" were tasked to make an oil rig loose its stability and move off course by change the counter thrusters meaning the oil pipe could rupture and split if it moved over a certain distance back & forth. The device that controls the thrusters is a Siemens S7 -1200. The device is used in every area of manufacturing, nuclear power plants, car manufacturing, food production. Last year they showed how a container ship could be compromised in a test, it change its weight, ballast controls, and direction, causing it to eventually roll and loose it load.

Think… When designing a system, using 3rd party parts, think about security.
What controls can I put in place to reduce threats, how good is the security on the site I'm installing on, when I use this 3rd party part is it compromising / weakening the security of my system.

Why be concerned ?

Latest hacks

Tesla cars – Not only being stolen without using the key Fobs but people can make the car do emergency breaking, open close windows, open doors while your driving it from a tablet or laptop !

https://www.youtube.com/watch?v=c1XyhReNcHY

Stuxnet Nuclear power plant – The virus that save the world from nuclear disaster, a usb pen was entered into an Iranian nuclear power system, it infected the siemens logical control modules and made the nuclear enrichment modules spin erratically making them fail over and over again disrupting their nuclear program for years. IT has found 5 years later !!. Was this government espionage or a disgruntled employee !?

https://www.youtube.com/watch?v=7g0pi4J8auQ

Companies changing to capitalise on hackers "Don't beat them join them"

The IT security world is changing. Now manufacturers are becoming more open and offering rewards. They want to test people and see if they can break into their product as they are realising the damage after is detrimental to their brand name, their profit and integrity.

$900,000 On Offer For Anyone Who Can Hack A Tesla Model 3

Thomas Brewster Forbes Staff
Cybersecurity
I cover crime, privacy and security in digital and physical forms.

A Tesla Model 3 on show. Will hackers be able to expose its weaknesses this March? 2018 THE DENVER POST, MEDIANEWS GROUP

Think you can hack a Tesla? Now's your chance. And you could win more than $900,000 in the process.

Google Offers $3.14159 Million In Total Rewards For Chrome OS Hacking Contest

Andy Greenberg Forbes Staff
Security
Covering the worlds of data security, privacy and hacker culture.

Google has never been stingy when it comes to paying for information about security vulnerabilities in its products. Now it's offering an especially large--and especially nerdy--sum of money.

At its third Pwnium hacking competition in Vancouver in March, the company is ponying up a total of $3.14159 million in prizes for hackers who can demonstrate critical security vulnerabilities in its Chrome OS operating system running on a Samsung Series 5 550