OWASP

The Open Web Application Security Project

from SCADA to IoT
Cyber Security

Bogdan Matache - Romania 2015

- **About ME, Bogdan Matache**
- Cyber Security Specialist – Military Technical Academy
- SCADA Security Specialist – InfoSec Institute
- Auditor – ISO 27001

Specializations: Cryptography, Social Engineering, SCADA Pen testing

- IT&C – over 15 y
- Energy @ OIL Sectors – 10 y
- SCADA for Renewable Power Plants – 5 y
- Pen testing – OIL Sectors systems – 3 y
- Pen testing – Electrical Systems – 3 y

What I hacked ?

- Fuel Pump (I changed densitometers values)

What I hacked ?

- Asphalt Station

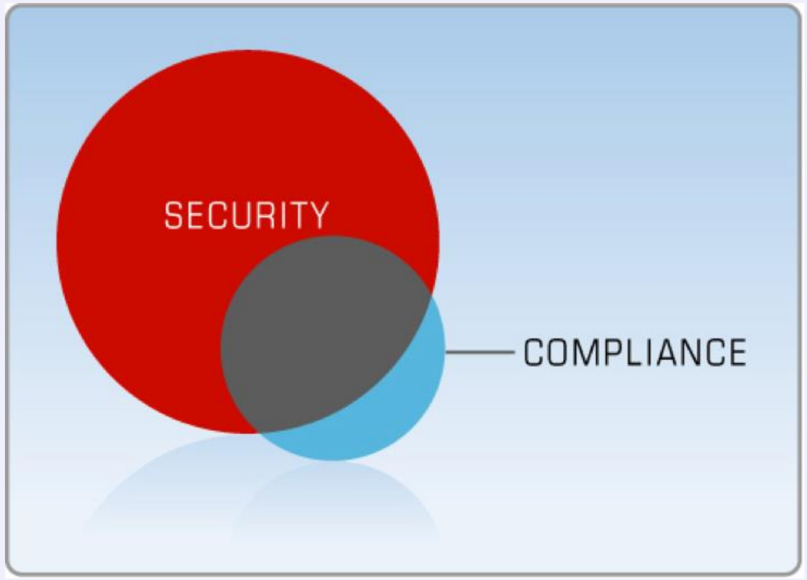
(I Changed the percentage of bitumen)

What I Pen Tested ?

- VoIP Networks
- WiMAX BTS
- Cars (doors open system, tachometer, gps)
- Intelligent House System, Smart Buildings
- 6 companies in 8 months (Social Engineering)
- PLC’s (programmable logic Controller)
- Smart Electricity Meters
- Smart Gas Meters
- Magnetic & RFID Access Cards
- Drones Control System
- Etc.

What I do ?

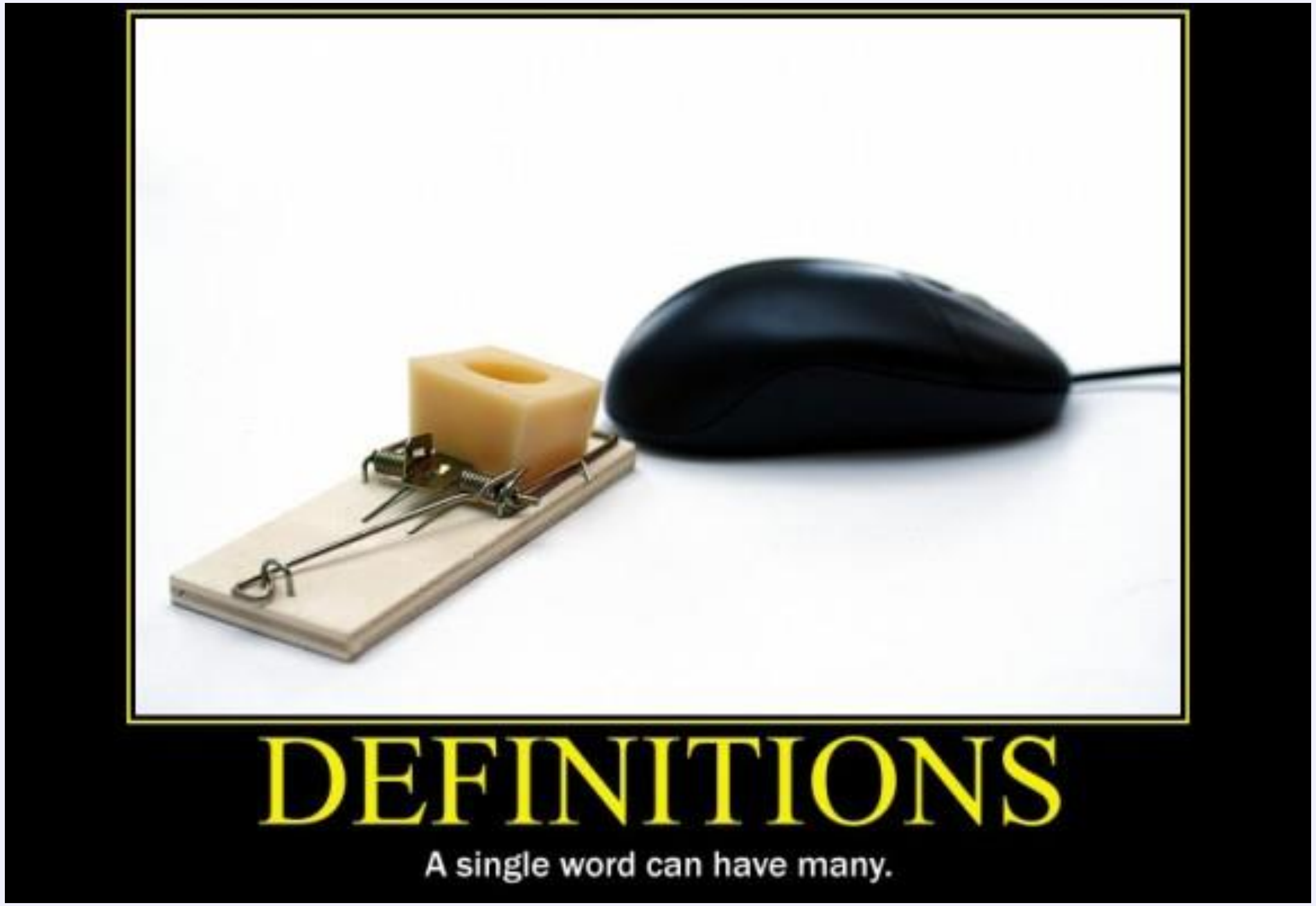
- I work as a security auditor at EnerSec, a company specialized in Cyber Security for Energy Sector



ENERSEC

Definitions

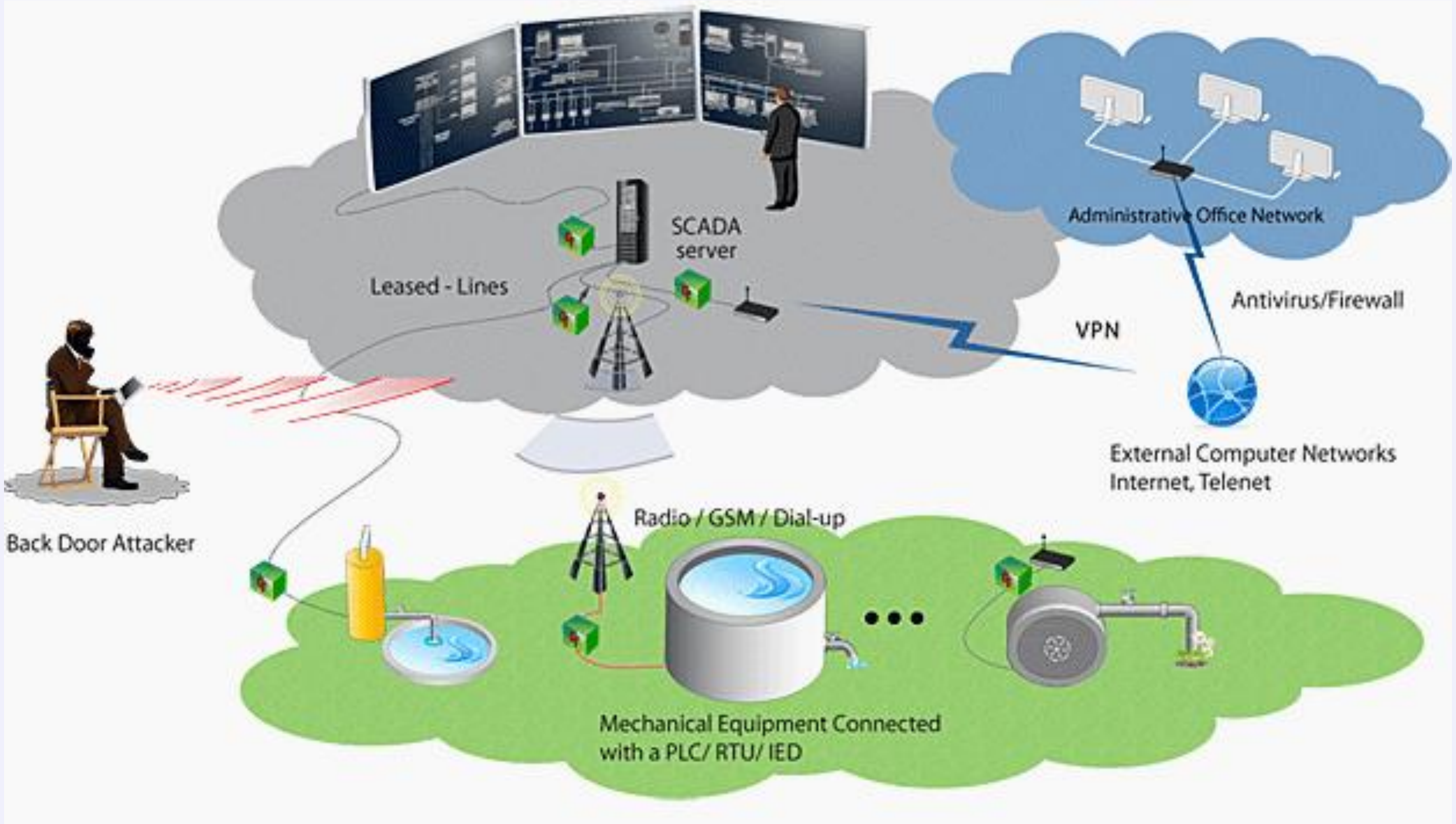
- What is SCADA
- What is IoT
- What is Security



ICS and SCADA

- Industrial Control Systems (ICS) is an umbrella term covering many historically different types of control system such as SCADA (Supervisory Control and Data Acquisition) and DCS (Distributed Control Systems). Also known as IACS (Industrial Automation and Control Systems), they are a form of Operational Technology. In practice, media publications often use “SCADA” interchangeably with “ICS”.

SCADA system

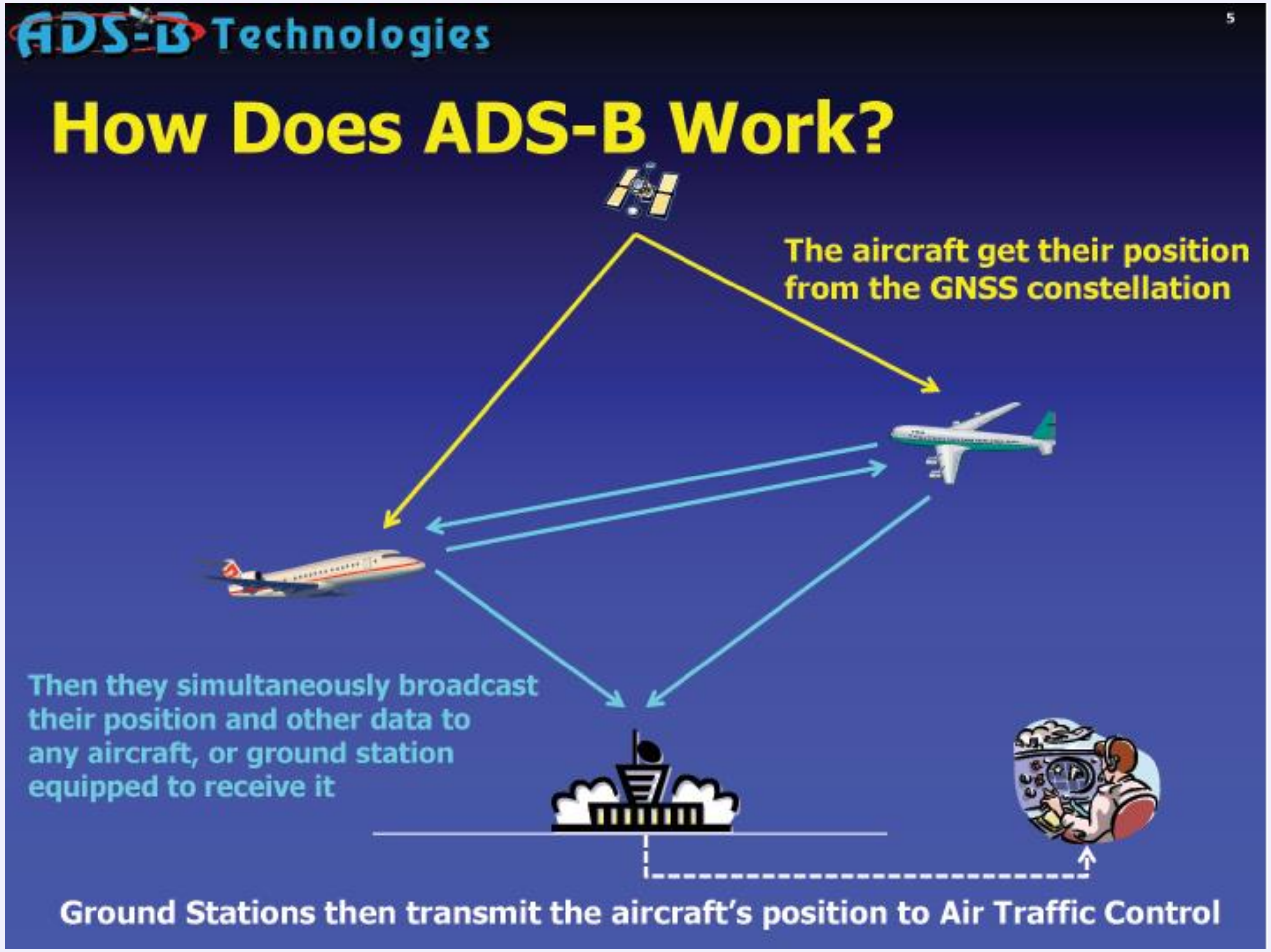


Cars

- OBD 2 (On-Board Diagnostics)

Airplanes

- ADS-B (Automatic Dependent Surveillance Broadcast)



ADS-B Technologies

5

How Does ADS-B Work?

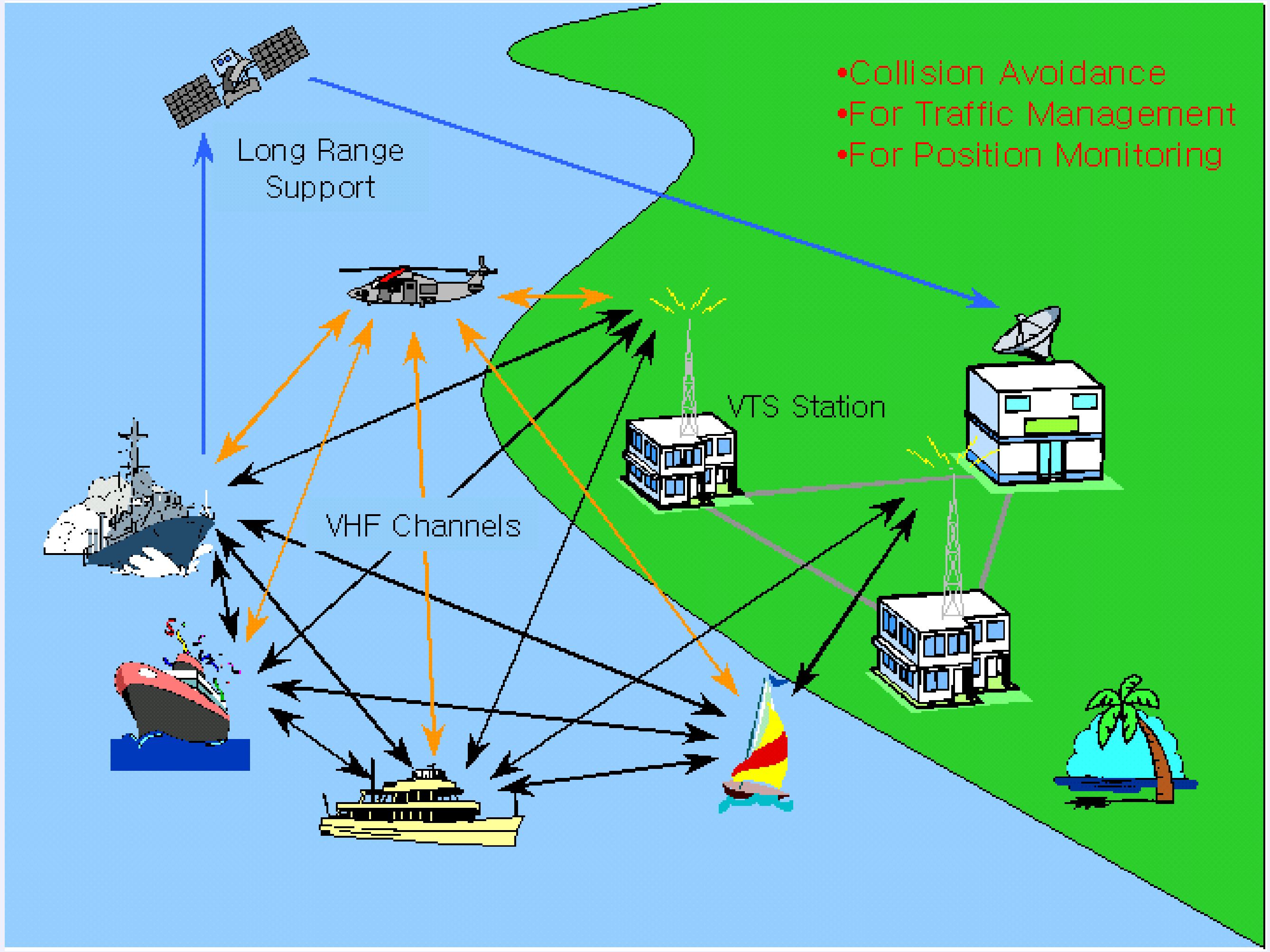
The aircraft get their position from the GNSS constellation

Then they simultaneously broadcast their position and other data to any aircraft, or ground station equipped to receive it

Ground Stations then transmit the aircraft's position to Air Traffic Control

Ships

- AIS (Automatic
  Identification
  System)



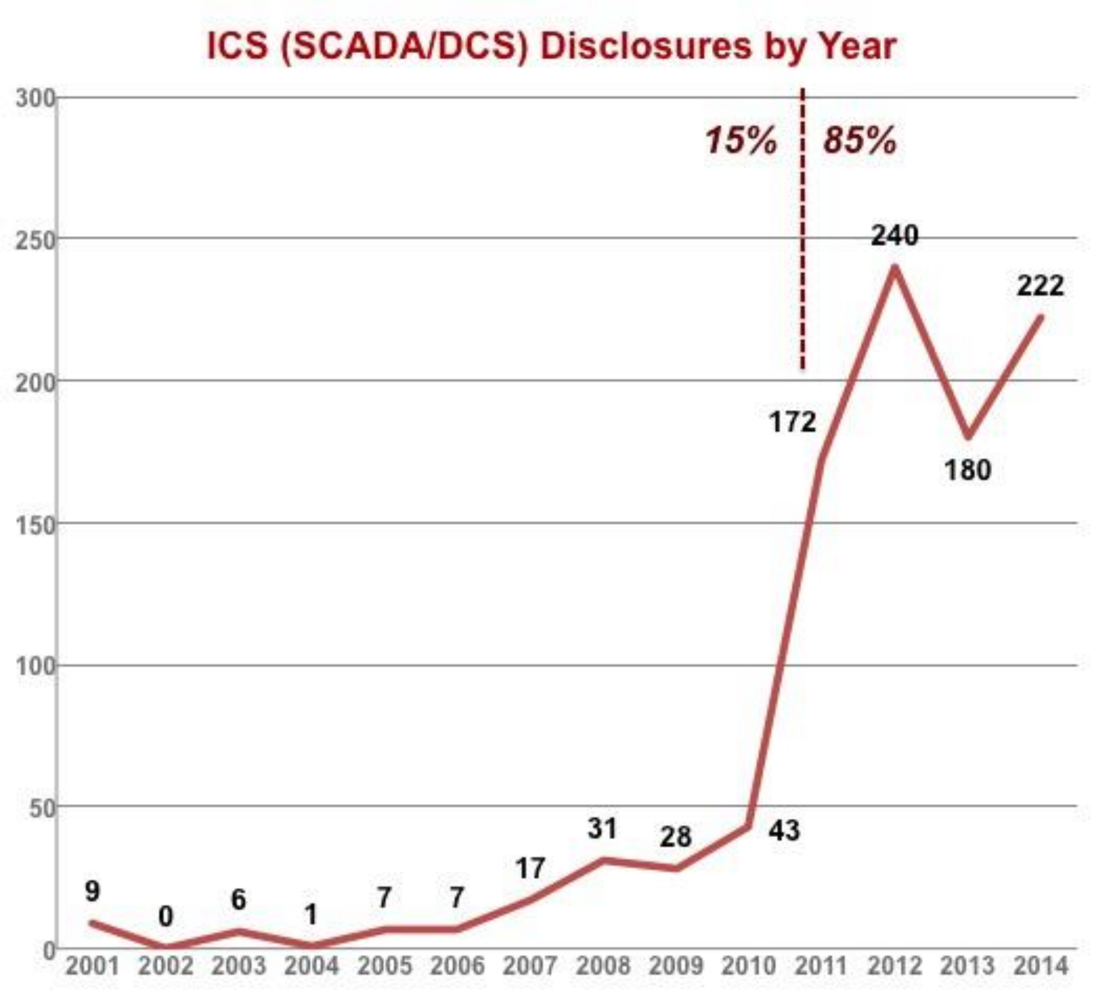
•Collision Avoidance
•For Traffic Management
•For Position Monitoring

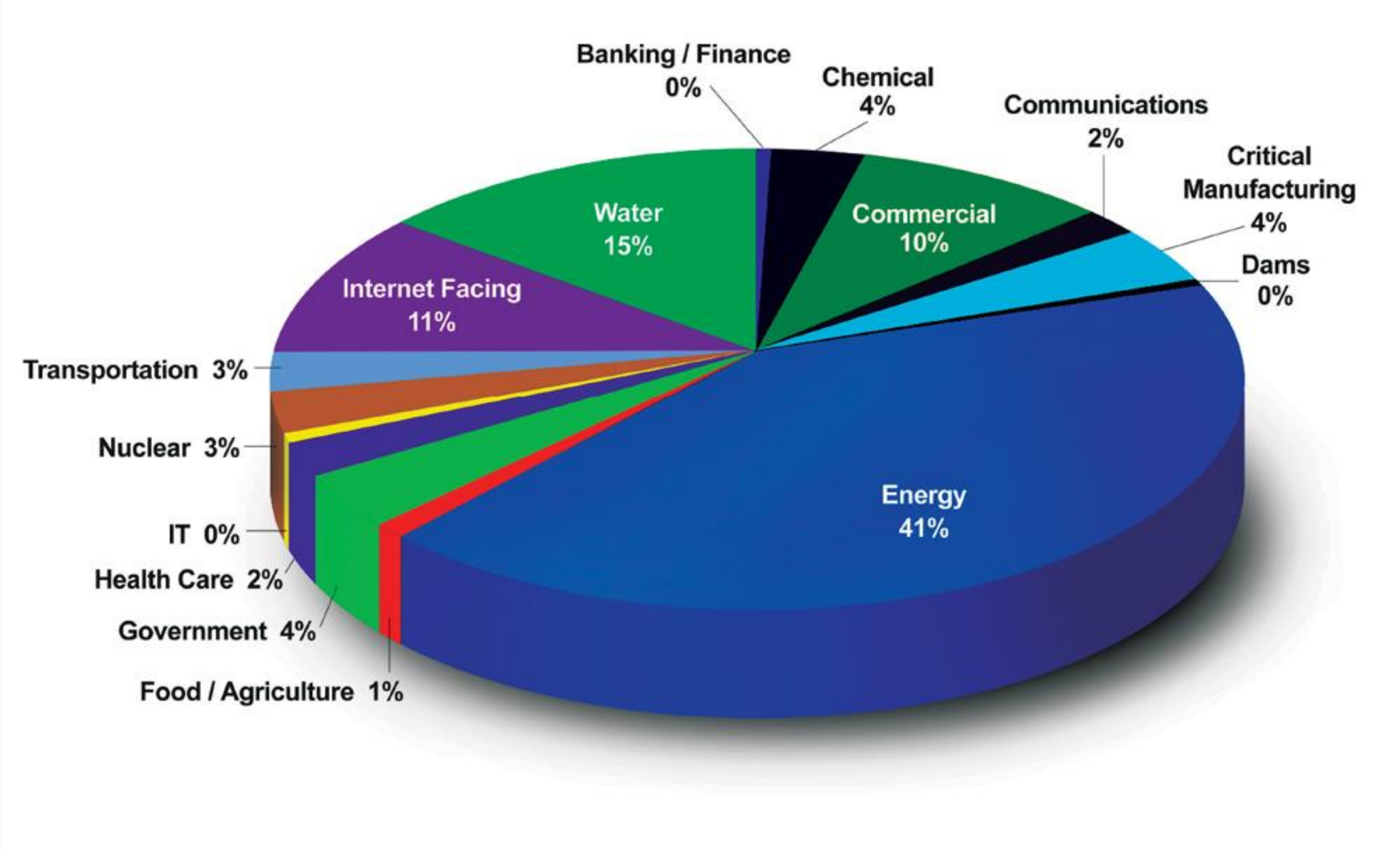
Other hackable SCADA systems

- Power Plants (Nuclear Plants)
- Transportation System

  (Train Switch Crossing and Beacons)
- Robots in factories
- Etc.

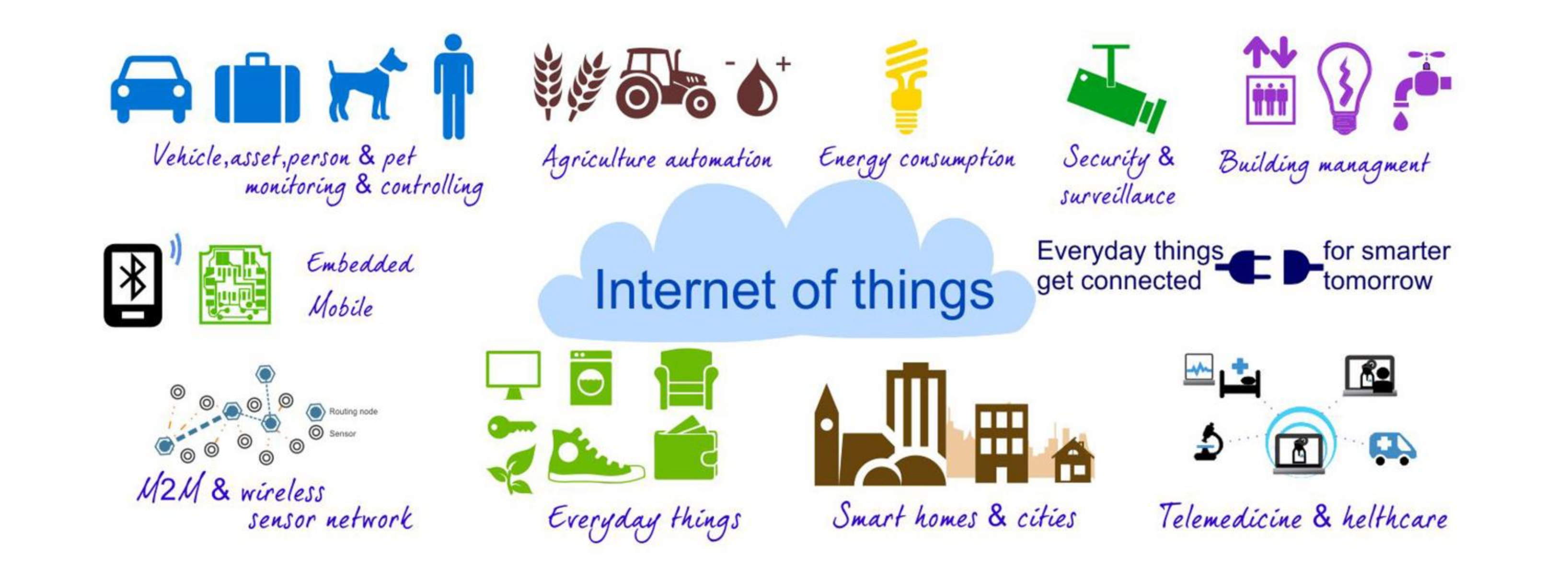
ics-cert.us-cert.gov



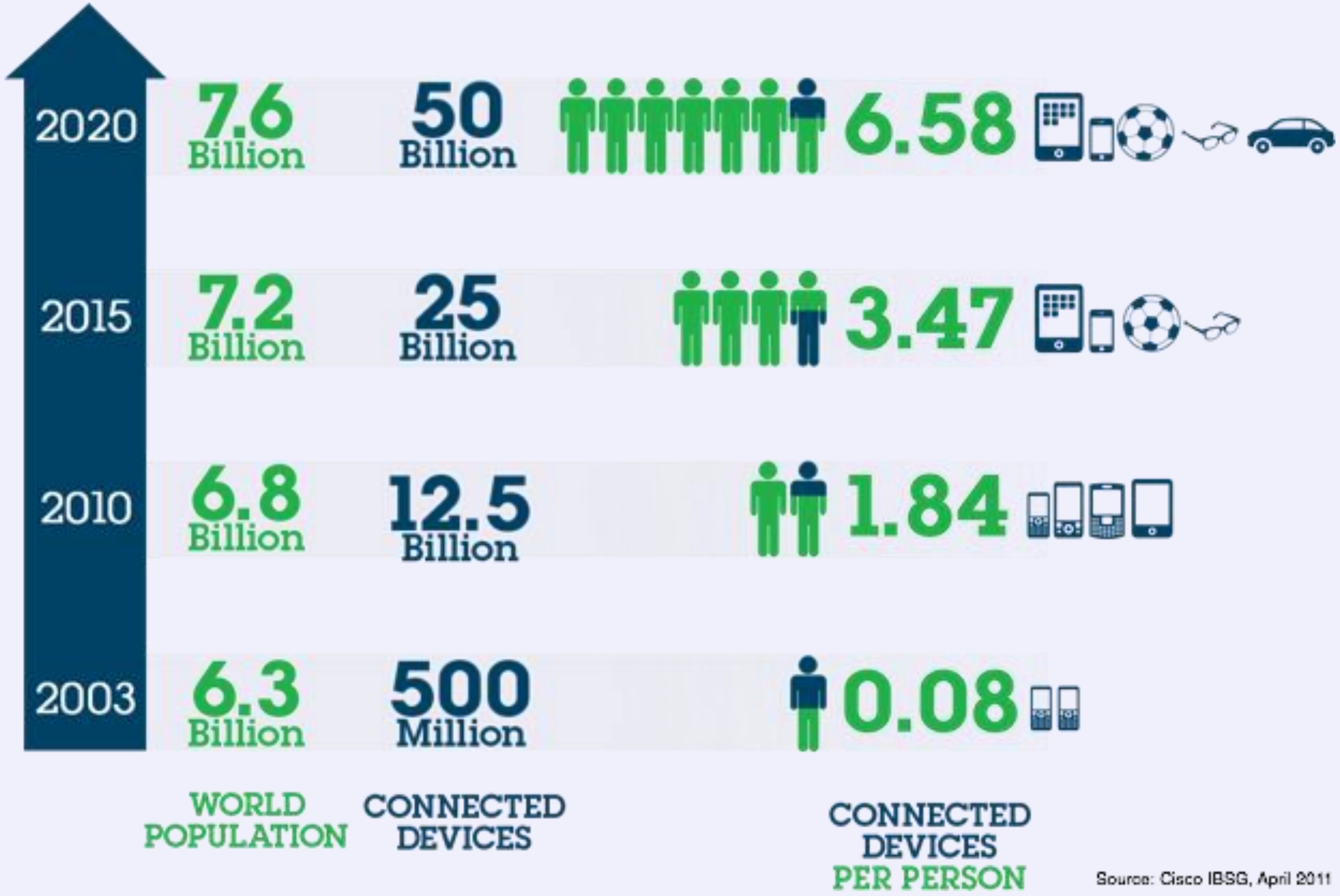

Banking / Finance 0%
Chemical 4%
Communications 2%
Critical Manufacturing 4%
Dams 0%
Commercial 10%
Water 15%
Internet Facing 11%
Transportation 3%
Nuclear 3%
IT 0%
Health Care 2%
Government 4%
Food / Agriculture 1%
Energy 41%

- The **Internet of Things** (IoT) is the network of physical objects or "**things**" embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data.

What is IoT ?



IoT Growth



	WORLD POPULATION	CONNECTED DEVICES	CONNECTED DEVICES PER PERSON
2020	7.6 Billion	50 Billion	6.58
2015	7.2 Billion	25 Billion	3.47
2010	6.8 Billion	12.5 Billion	1.84
2003	6.3 Billion	500 Million	0.08

Source: Cisco IBSG, April 2011

SCADA vs IoT

- More devices
- More Systems
- More data
- More connectivity / access points
- More ‘home’ users

- Equals - More opportunities

Attacks Types for SCADA

- Power System or Water System (most likely terrorism)

- *Attacks upon the power system*.

  target – power system itself
- *Attacks by the power system*.

  target – population (make dark or rise lever of chlorine)
- *Attacks through the power system*

  target - ex high voltage for a specific company

Attacks types for IoT

- Open doors (Bluetooth Lockers, hotel rooms)
- Unwanted Surveillance (baby monitors or smart TV's)
- Damage things (Sprinklers, cooling systems)

- Pace Maker

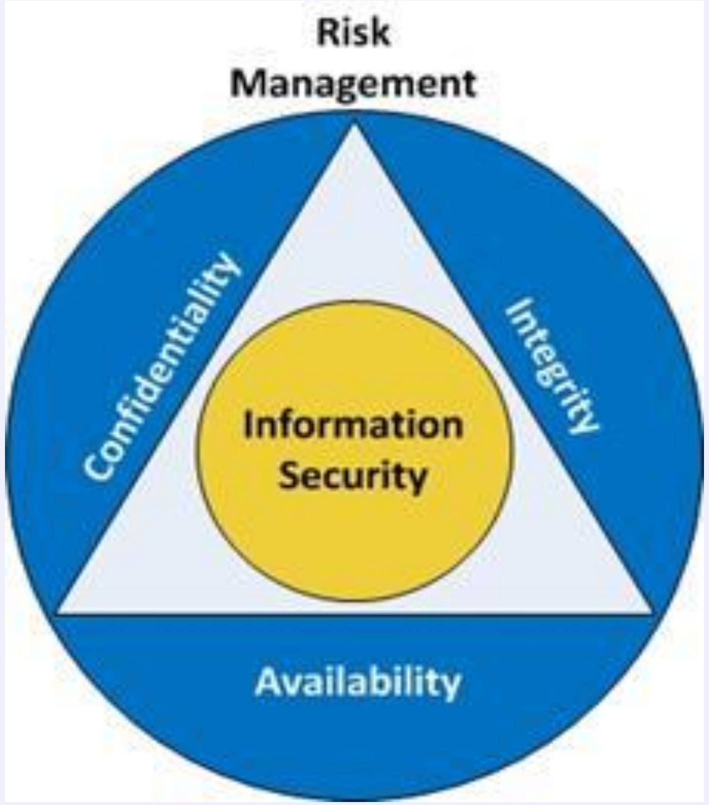
- GPS (fleet monitoring)

- Burglars (profile from smart meters, energy consumption)

2015 SECURITY PREDICTIONS
Symantec.
#1 ATTACKS ON THE INTERNET OF THINGS WILL FOCUS ON SMART HOME AUTOMATION

CIA vs AIC

- IT Security
  confidentiality, integrity, availability
- SCADA and IoT
  availability, integrity, confidentiality



Protocols

- **For SCADA (PLC's)**

  ModBus, DNP3, IEC 60870, IEC61850, Embedded Proprietary, ICCP, UCA 2.0

- **For IoT**

  Bluetooth low-e, Wi-Fi low-e, NFC, RFID, ANT, Z-Wave, Neul, SigFox, Thread, 6LowPAN, ZigBee, Cellular, LoRA WAN

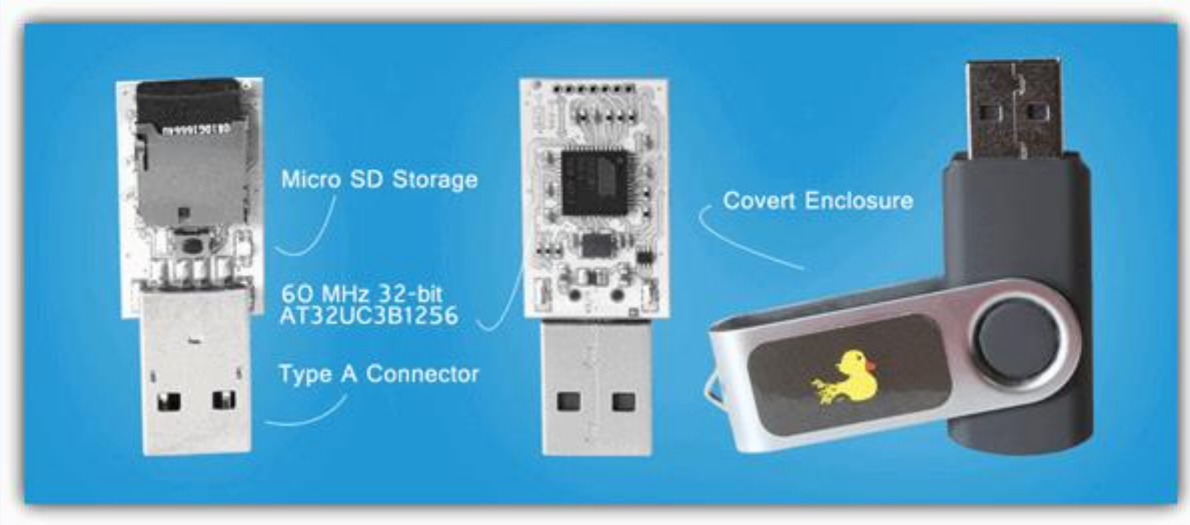
Software for Hacking SCADA / IoT

- Black Arch Linux
- Hack Ports
- Helix, Kali Linux
- Samurai STFU
- Security Onion
- OSINT
- Dedicated software exploits for PLC's

for Siemens, Allen Bradley, Schneider, ABB, etc.

Hardware tools for Pentest

- WiFi Pineapple
- Rubber Ducky



Hardware tools for Pentesting

- Hack RF

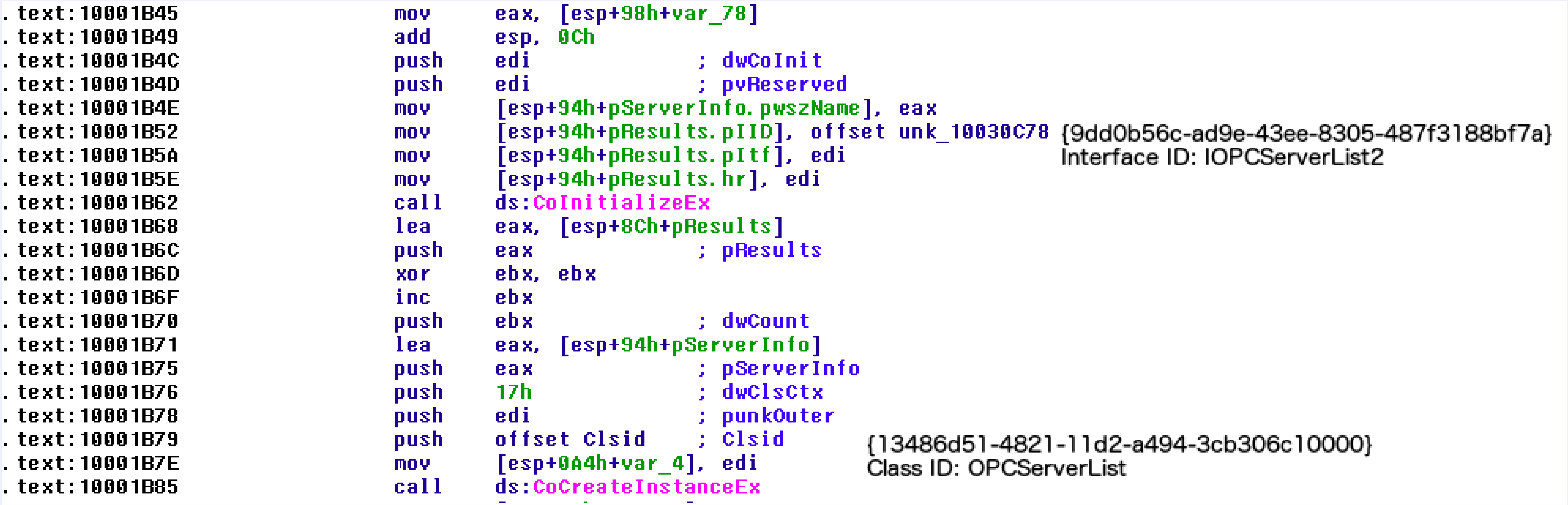
Hardware tools for Pentest

- Prox Mark 3

  clone RFID Mifare cards

Malware example for SCADA / IoT

- Stuxnet, Havex, Flame, DragonFly
- APT is most dangerous



```
.text:10001B45                 mov     eax, [esp+98h+var_78]
.text:10001B49                 add     esp, 0Ch
.text:10001B4C                 push    edi             ; dwCoInit
.text:10001B4D                 push    edi             ; pvReserved
.text:10001B4E                 mov     [esp+94h+pServerInfo.pwszName], eax
.text:10001B52                 mov     [esp+94h+pResults.pIID], offset unk_10030C78 {9dd0b56c-ad9e-43ee-8305-487f3188bf7a}
                                                                                    Interface ID: IOPCServerList2
.text:10001B5A                 mov     [esp+94h+pResults.pItf], edi
.text:10001B5E                 mov     [esp+94h+pResults.hr], edi
.text:10001B62                 call    ds:CoInitializeEx
.text:10001B68                 lea     eax, [esp+8Ch+pResults]
.text:10001B6C                 push    eax             ; pResults
.text:10001B6D                 xor     ebx, ebx
.text:10001B6F                 inc     ebx
.text:10001B70                 push    ebx             ; dwCount
.text:10001B71                 lea     eax, [esp+94h+pServerInfo]
.text:10001B75                 push    eax             ; pServerInfo
.text:10001B76                 push    17h             ; dwClsCtx
.text:10001B78                 push    edi             ; punkOuter
.text:10001B79                 push    offset Clsid    ; Clsid        {13486d51-4821-11d2-a494-3cb306c10000}
.text:10001B7E                 mov     [esp+0A4h+var_4], edi          Class ID: OPCServerList
.text:10001B85                 call    ds:CoCreateInstanceEx
```

Critical risk scenarios

- RS 01 - **disrupting the operation of control systems** by delaying or blocking the flow of information through control networks, thereby denying availability of the networks to control system operators;

- RS 02 - **unauthorized changes to programmed instructions** in PLCs, RTUs, or DCS controllers, change alarm thresholds, or issue unauthorized commands to control equipment, which could potentially result in damage to equipment (if tolerances are exceeded), premature shutdown of processes (such as prematurely shutting down transmission lines), or even disabling control equipment;

Critical risk scenarios

- RS 03 - **send false information to control system** operators either to disguise unauthorized changes or to initiate inappropriate actions by system operators;
- RS 04 - **modify the control system software**, producing unpredictable results;
- RS 05 - **interfere with the operation** of safety systems.

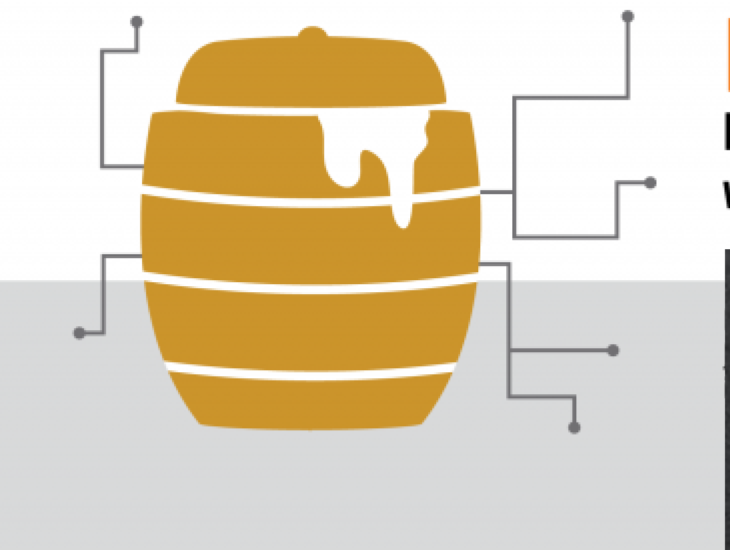
Defence / Alerts

- ***ics**-**cert***.*us-**cert**.gov*
- CERT-ICS.eu

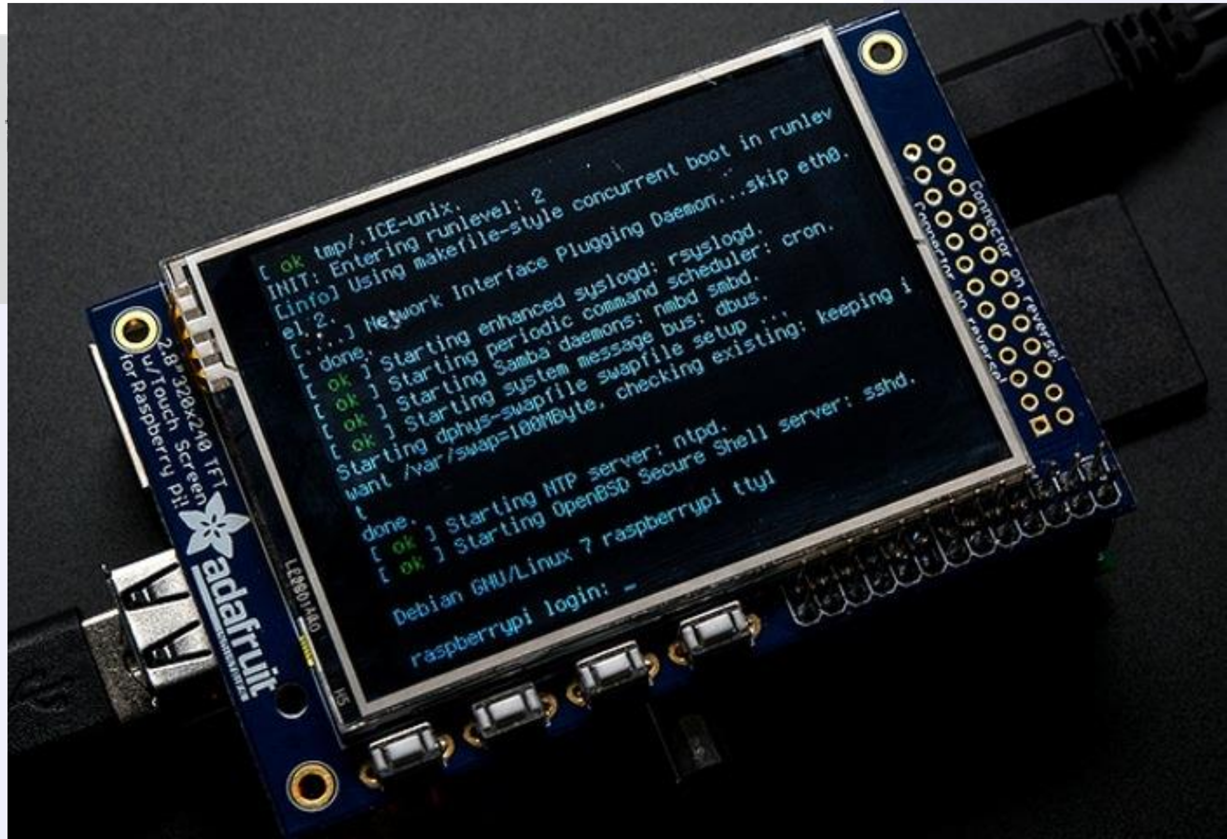
U.S. DEPARTMENT OF HOMELAND SECURITY

INDUSTRIAL CONTROL SYSTEMS
CYBER EMERGENCY RESPONSE TEAM

OWASP
The Open Web Application Security Project



HACKING BACK:
Proactive Threat Intelligence
with Honeypots for Active Defense



```
[ ok  tmp/.ICE-unix.
INIT: Entering runlevel: 2
[info] Using makefile-style concurrent boot in runlev
el 2.
[....] Network Interface Plugging Daemon...skip eth0.
 done.
[ ok ] Starting enhanced syslogd: rsyslogd.
[ ok ] Starting periodic command scheduler: cron.
[ ok ] Starting Samba daemons: nmbd smbd.
[ ok ] Starting system message bus: dbus.
Starting dphys-swapfile swapfile setup ...
want /var/swap=100MByte, checking existing: keeping i
t
done.
[ ok ] Starting NTP server: ntpd.
[ ok ] Starting OpenBSD Secure Shell server: sshd.

Debian GNU/Linux 7 raspberrypi tty1

raspberrypi login: _
```

Defence / Intelligence

Security Operation Center

Q
&
A

рахмат
danke
謝謝
ngiyabonga
teşekkür ederim
Баярлалаа
спасибо
mersi
kia ora
barka
welalin
tack
spas
mahalo
tapadh leat
faafetai lava
vinaka
blagodaram
dank je
misaotra
matondo
paldies
grazzi
kiitos
dankie
спасибі
хвала
thank you
gracias
dhanyavad
nanni
nandri
maururu
köszönöm
asante
manana
obrigada
tenki
bedankt
bayarlalaa
gràcie
hvala
akun
dankon
aciū
djiere dieuf
tau
mochchakkeram
murakoze
дякую
mamnun
chokrane
enkosi
dziękuję
chnorakaloutioun
gratias ago
gràcies
sulpáy
go raibh maith agat
taiku
sobodi
dêkuji
sukriya
kop khun krap
sagolun
obrigado
mèsi
didi madloba
najis tuke
ありがとう
tanemirt
grazie
arigatô
takk
dakujem
trugarez
kam sah hamnida
rahmat
terima kasih
rahmet
ευχαριστώ
diolch
dhanyavadagalu
shukriya
mercè
мерси
তোমাকে ধন্যবাদ
감사합니다
xièxie
merci