IOActive™

COMPREHENSIVE COMPUTER SECURITY SERVICES

Northwestern Passages
NU
Hudson Bay
MB
ON
QC
NL
Gulf of St Lawrence
ND
SD
NE
KS
MO
TX
LA
TN
NC
SC
MD
DE
NJ
CT
RI
MA
NH
NS
NB
PE
Gulf of
Greenland
Iceland
North Atlantic Ocean
Norwegian Sea
Sweden
North Sea
Ireland
Bay of Biscay
Portugal
Spain
Morocco
Algeria
Tunisia
Libya
Egypt
Mediterranean Sea
Greece
Turkey
Syria
Iraq
Iran
Ukraine
Turkmenistan
Afghani
Uzbekista
Kazak

The last gasp of the industrial air gap…

Éireann Leverett

BEng MPhil CSSLP CSSA ISEB

Airgap myths

- They are the default in industrial systems
  - I have more than 12k counter-examples for ICS
  - 22K more for HVAC and BMS
- They are easy to deploy and maintain
  - Networks aren’t static, they change over time
- They are cheap
  - They restrict business drivers like cross org info sharing
- They make attacks impossible
  - Stuxnet showed this is not the case
  - There are many insider or physical attacks that bridge air-gaps
  - Then you are soft and exposed, because you didn’t push AppSec

Industrial Control Systems

- How many are internet facing?
  - How do we measure that?

SHODAN

Scans the entire IPv4 space
~Every 3 months
Logs banners on ports:
21, 22, 23, 80, 161, 443

My Code:

Using 52 popular ICS products
We search the two year database for hits
Then we geolocate them

My Code:

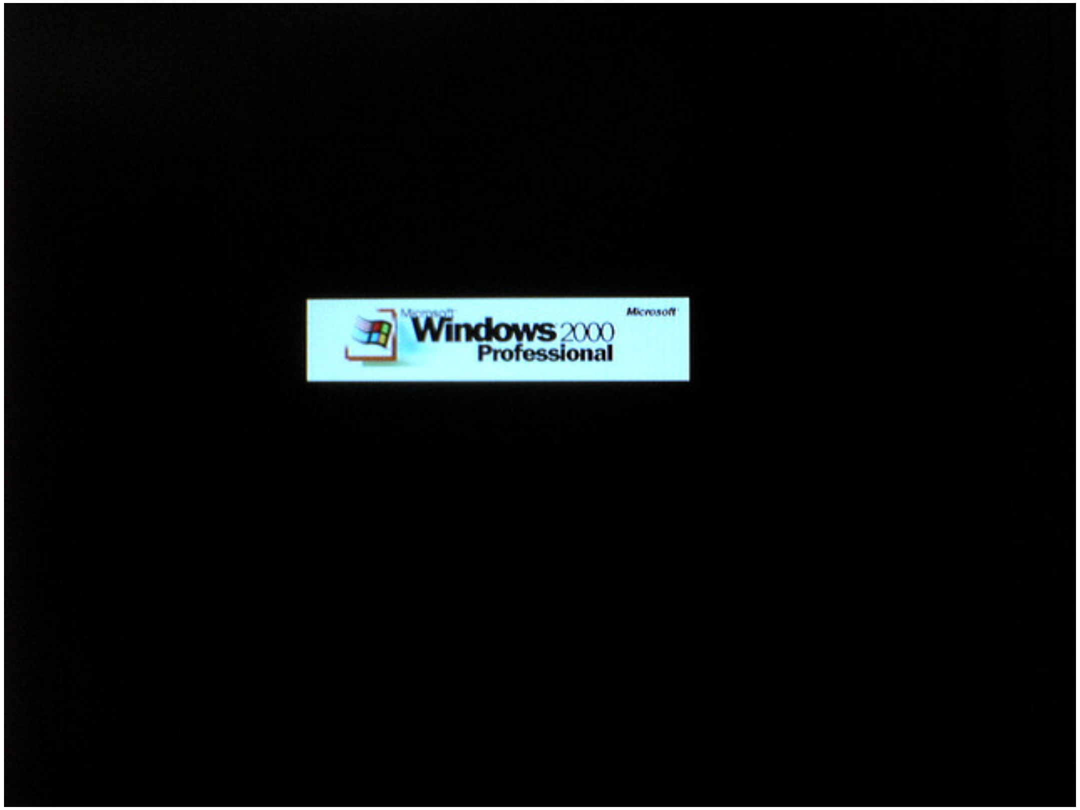
Finally we decompose the banners and search for common or known exploits based on version numbers

Back in 2002…

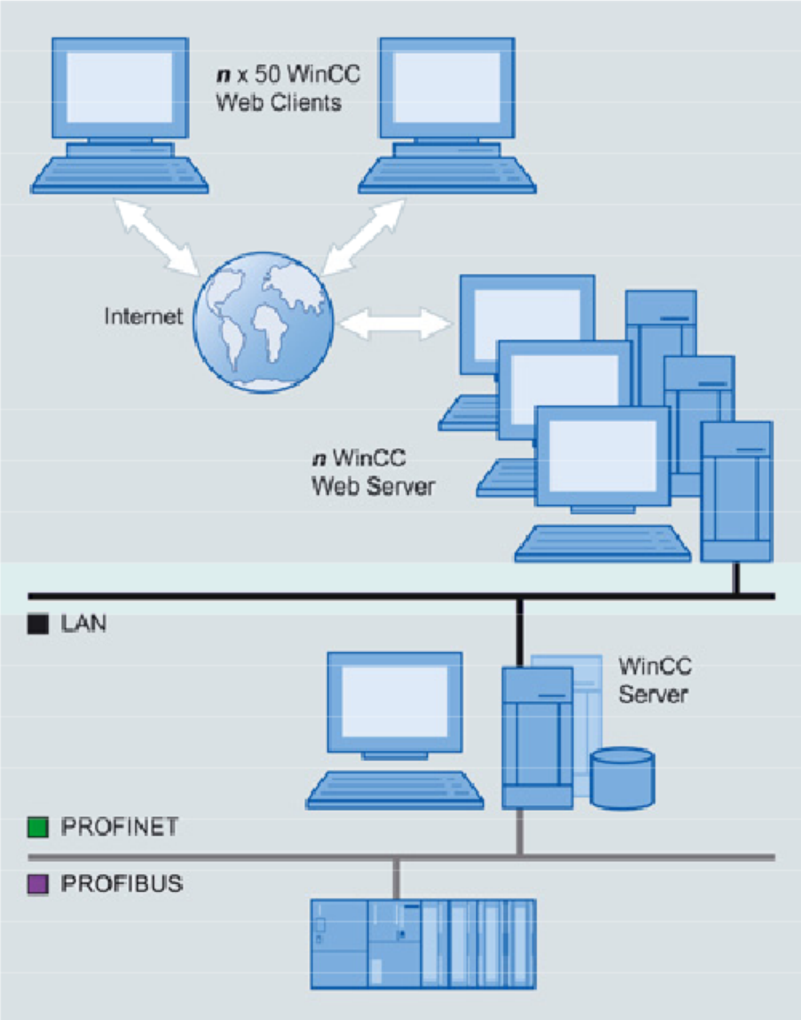
“Trustworthy Computing is computing that is as available, reliable and secure as electricity, water services and telephony.”

Trustworthy Computing is a success then!

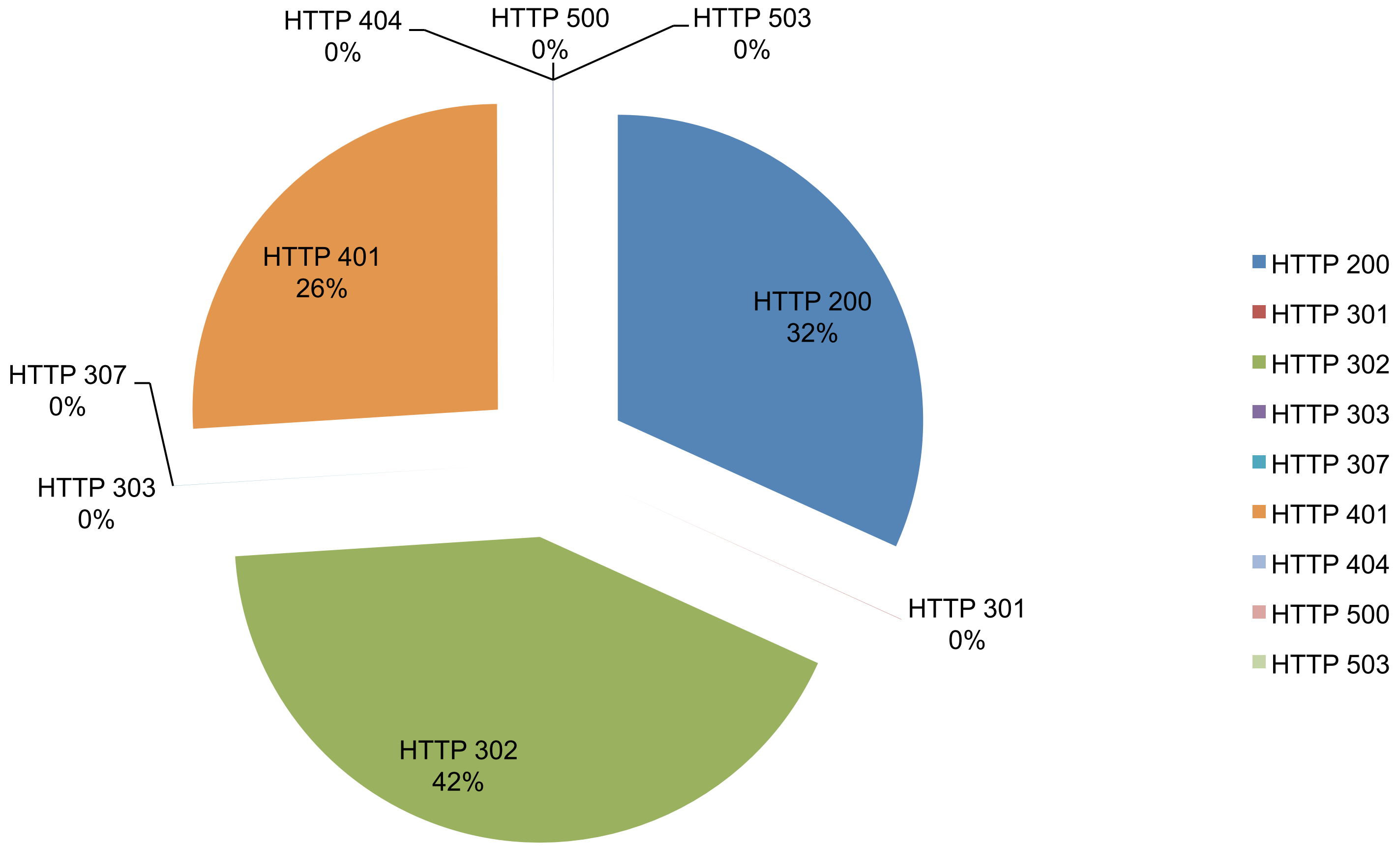
Because the most popular OS I found was….



I RTFM.


n x 50 WinCC Web Clients
Internet
n WinCC Web Server
■ LAN
WinCC Server
🟩 PROFINET
🟪 PROFIBUS

Can’t air-gap? Use HTTP 401 at least!



IOActive™

COMPREHENSIVE COMPUTER SECURITY SERVICES

What did I just tell you?
We are statistically failing....

- 22K Building Management Systems and
- 12K Industrial Control and UPS Systems and Devices
- Can be found in Shodan’s results with 52 queries
- Only 26% of the HTTP responses INIT to Auth
- 53% of had REMOTE vulns in ExploitDB or Metasploit
- I don’t pull LOCAL cause I already suffer SLEEPFAILS
- Many leak info like default passwords in HELP FILES
- LOL, WAT?
- Passwords.
- In 2012.
- For companies who sell “Critical National Infrastructure”.
- Find me at parties for LULZY screenshots!

What air-gap? It’s roll up your sleeves time.

BY NC SA ©Beck Tench - 2011-01-09 18:03:18
www.flickr.com/92397015@N00/5340350175/

Email:	eireann (.) leverett [AT] ioactive (dot) co (dot) uk
Twitter:	@blackswanburst
PGP:	C97C1513