Denial of Surface.

Eireann Leverett
MPhil BEng CSSA CSSLP ISEB
@blackswanburst
eireann.leverett@cantab.net

Overview

- On the nature of criticality
- The Scanning Problem
- Shodan-FU
- The Patching Problem
- Exploits
- Geolocation
- Data Analysis
- Conclusions

On the nature of criticality…

- I hate the phrase:
- ‘critical national infrastructure’

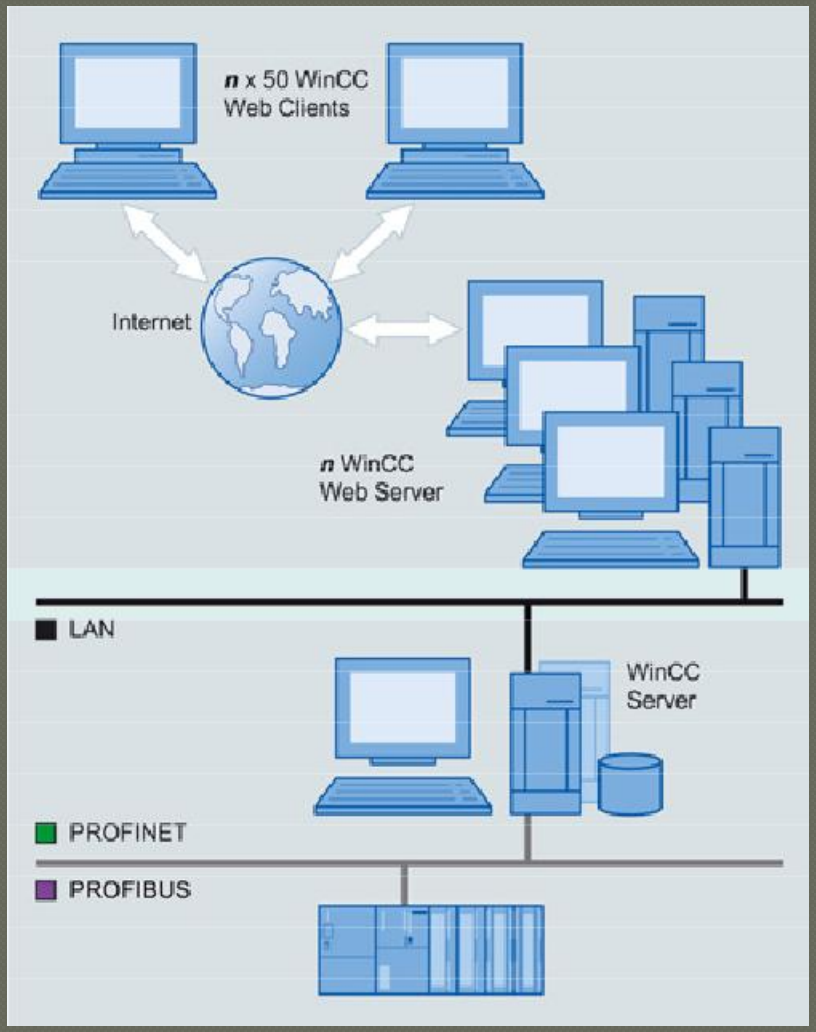
- Critical infrastructure may not be in country
- Criticality varies over time
- Criticality varies by numbers

- Is HVAC Critical?

The airgap is dead.

- This is presentation is about physical systems, directly on the internet.
- No need for firewalking.
- They're directly on the internet.
- Why?
- Business drivers. Understand them.
- The CSO needs to challenge the CFO
- Cost cutting can increase risk.

I RTFM.


n x 50 WinCC
Web Clients
Internet
n WinCC
Web Server
LAN
WinCC
Server
PROFINET
PROFIBUS

One product for HVAC/BMS

- Niagara Web Server
- Tridium
- Lots of different integrators
- 15,535 results globally
- 12,659 in the US alone
- People say HVAC and BMS isn't critical…
- Hospitals? Subways? Control rooms?
- How abut we look at a few here in DC…

Some ‘motivating’ Examples

- 65.207.77.213/login
- Somerset County Health
- IP2Location gives us 38.9048, -77.0354
- Which is probably the ISP
- Or
- 216.15.32.84/login
- 70.21.118.209/login
- 75.145.84.164/login
- Let’s look at all of them!

The scanning problem

What does Shodan do?

- Scan All IPv4 addresses.
- Use web or API (Protip: API has more info)
- Can export XML result sets from web
- Ports:
  - 21 - FTP
  - 22 - SSH
  - 23 - Telnet
  - 80 - HTTP
  - 161 - SNMP
  - 443 - HTTPS

Shodan queries I use

- Modicon+M340+CPU
- PowerLink
- HMS+Anybus-S+WebServer
- NovaTech+HTTPD
- Modbus+Bridge
- Cimetrics+Eplus+Web+Server
- A850+Telemetry+Gateway
- CitectSCADA
- i.LON
- EIG+Embedded+Web+Server
- TAC/Xenta
- WAGO
- ConnectUPS
- MOXA
- Moscad
- Telemecanique
- **/gc/flash.php**
- HMI_Panel port:23

- /BroadWeb/
- ioLogik
- Carel PlantVisor
- SoftPLC
- EnergyICT
- RTU560
- eiPortal
- RTS+Scada
- Simatic+HMI
- Simatic+S7
- SIMATIC+NET
- CIMPLICITY
- webSCADA-Modbus
- ModbusGW
- Allen-Bradley
- Reliance+4+Control+Server

The patching problem: FOREVERDAY

Sample Banner Decomposition

- HTTP/1.0 401 Authorization Required
- Date: Mon, 07 Feb 2011 21:45:24 GMT
- Server: Apache/2.0.63 (FreeBSD) mod_python/3.3.1 Python/2.5.1
- WWW-Authenticate: Digest realm="RTS SCADA Server", nonce="igs8JribBAA=f2dc6be74835f4f9ea3b591bdd839834771a8494", algorithm=MD5, domain="/ http://vZNX.fieldlinq.com/", qop="auth"
- Content-Length: 401
- Content-Type: text/html; charset=iso-8859-1
- Via: 1.1 znx.fieldlinq.com
- Vary: Accept-Encoding

Banner Decomposition

- Apache/2.0.63 (FreeBSD) mod_python/3.3.1 Python/2.5.1

Banner Decomposition

- Apache/2.0.63 FreeBSD mod_python/3.3.1 Python/2.5.1

Banner Decomposition

- Apache 2.0.63 FreeBSD mod_python 3.3.1 Python 2.5.1

Banner Decomposition

Now they are exploit search terms:

- Apache 2.0.63
- FreeBSD
- mod_python 3.3.1
- Python 2.5.1

The Recipe

- SHODAN results
- A liberal dash of geolocation
- A pinch of regex and exploit searches
- A dash of visualisation.

- Now you can see the scale of the horror.

“We had the tools, we had the talent.”

Exploit

- New exploits come in daily
- (Hat Tip Reid, Ruben, Billy & Terry)
- SO VISUALISE IT.
- More accurate when done by hand
- Automation if you need it quickly
- Sources:
  - Exploit DB (Automatable)
  - Metasploit Project (Automatable)
  - OSVDB (Non Auto)

Geolocation

- I'm just using passive Geolocation
- It's good enough to help us mitigate
- Recent improvements to 690 meters
- If it gets better than that we have new problems
- Commercial databases are better
- But now John Matherly of SHODAN has incorporated it due to my research.

Here, take my eyes…

Conclusions

- The airgap is dead. Understand why.
- Beware the scanning problem.
- The long lifecycle is a key factor here.
- Known vulnerabilities & exploits.
- Criticality is not for us to judge.
- Synthesize data for Situational View.
- OWASP people have the skills.
- You just need to learn the domain
- JOIN US!

Questions


©LEOL30 - 2012-02-16 14:30:37
www.flickr.com/49968232@N00/6839982288/