Using SPA for profit and fun

Or

“a zero-cost solution to getting your fridge out of Shodan.”

Adrianus Warmenhoven

adrianus@warmenhoven.co

(not .com)

Privacy & Security Evangelist

(Security) Researcher (nay hacker)

Entrepreneur

The problem - 1

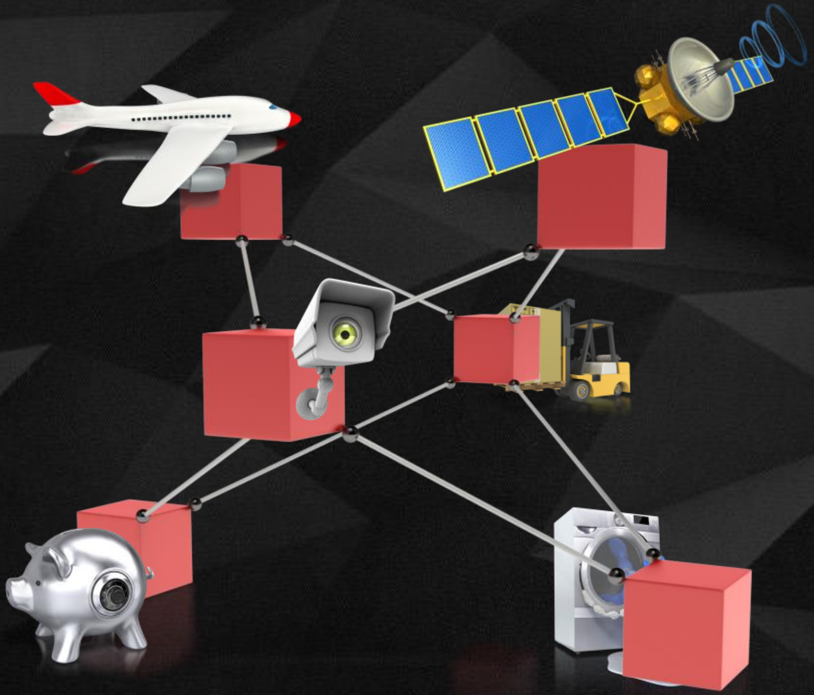
In the beginning:

The problem - 2

The global network

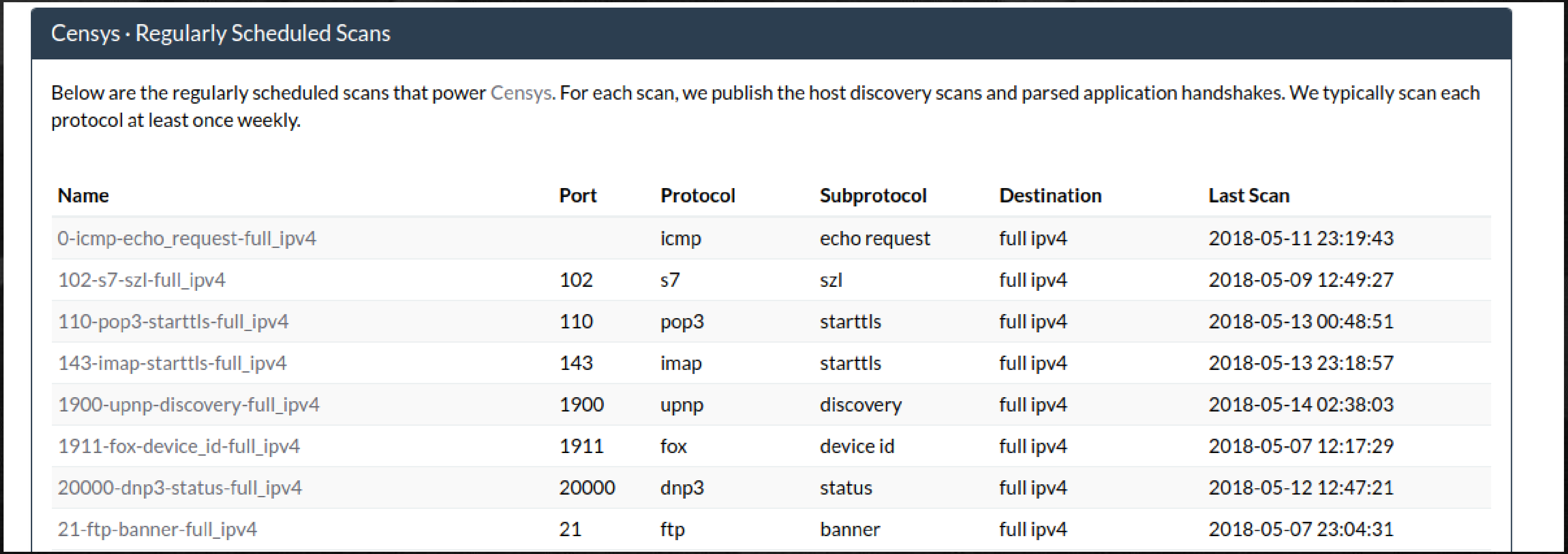
The problem - 3

When we say ‘smart’, we usually just mean ‘it has an IP address’



The problem - 4

scans.io (censys.io)



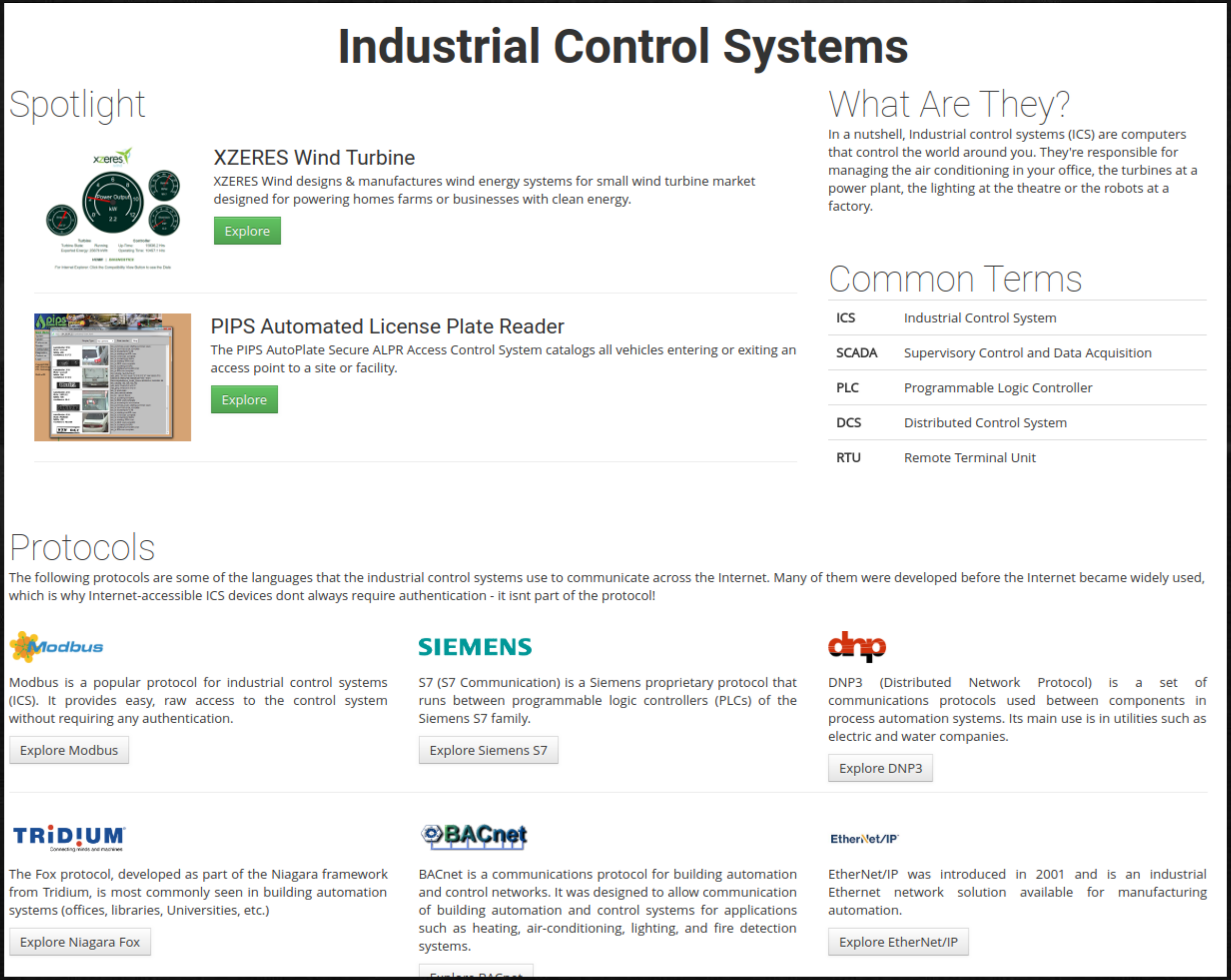
Censys · Regularly Scheduled Scans

Below are the regularly scheduled scans that power Censys. For each scan, we publish the host discovery scans and parsed application handshakes. We typically scan each protocol at least once weekly.

Name	Port	Protocol	Subprotocol	Destination	Last Scan
0-icmp-echo_request-full_ipv4		icmp	echo request	full ipv4	2018-05-11 23:19:43
102-s7-szl-full_ipv4	102	s7	szl	full ipv4	2018-05-09 12:49:27
110-pop3-starttls-full_ipv4	110	pop3	starttls	full ipv4	2018-05-13 00:48:51
143-imap-starttls-full_ipv4	143	imap	starttls	full ipv4	2018-05-13 23:18:57
1900-upnp-discovery-full_ipv4	1900	upnp	discovery	full ipv4	2018-05-14 02:38:03
1911-fox-device_id-full_ipv4	1911	fox	device id	full ipv4	2018-05-07 12:17:29
20000-dnp3-status-full_ipv4	20000	dnp3	status	full ipv4	2018-05-12 12:47:21
21-ftp-banner-full_ipv4	21	ftp	banner	full ipv4	2018-05-07 23:04:31

The problem - 5

shodan.io



Industrial Control Systems

Spotlight

XZERES Wind Turbine

XZERES Wind designs & manufactures wind energy systems for small wind turbine market designed for powering homes farms or businesses with clean energy.

PIPS Automated License Plate Reader

The PIPS AutoPlate Secure ALPR Access Control System catalogs all vehicles entering or exiting an access point to a site or facility.

What Are They?

In a nutshell, Industrial control systems (ICS) are computers that control the world around you. They're responsible for managing the air conditioning in your office, the turbines at a power plant, the lighting at the theatre or the robots at a factory.

Common Terms

ICS	Industrial Control System
SCADA	Supervisory Control and Data Acquisition
PLC	Programmable Logic Controller
DCS	Distributed Control System
RTU	Remote Terminal Unit

Protocols

The following protocols are some of the languages that the industrial control systems use to communicate across the Internet. Many of them were developed before the Internet became widely used, which is why Internet-accessible ICS devices dont always require authentication - it isnt part of the protocol!

Modbus is a popular protocol for industrial control systems (ICS). It provides easy, raw access to the control system without requiring any authentication.

S7 (S7 Communication) is a Siemens proprietary protocol that runs between programmable logic controllers (PLCs) of the Siemens S7 family.

DNP3 (Distributed Network Protocol) is a set of communications protocols used between components in process automation systems. Its main use is in utilities such as electric and water companies.

The Fox protocol, developed as part of the Niagara framework from Tridium, is most commonly seen in building automation systems (offices, libraries, Universities, etc.)

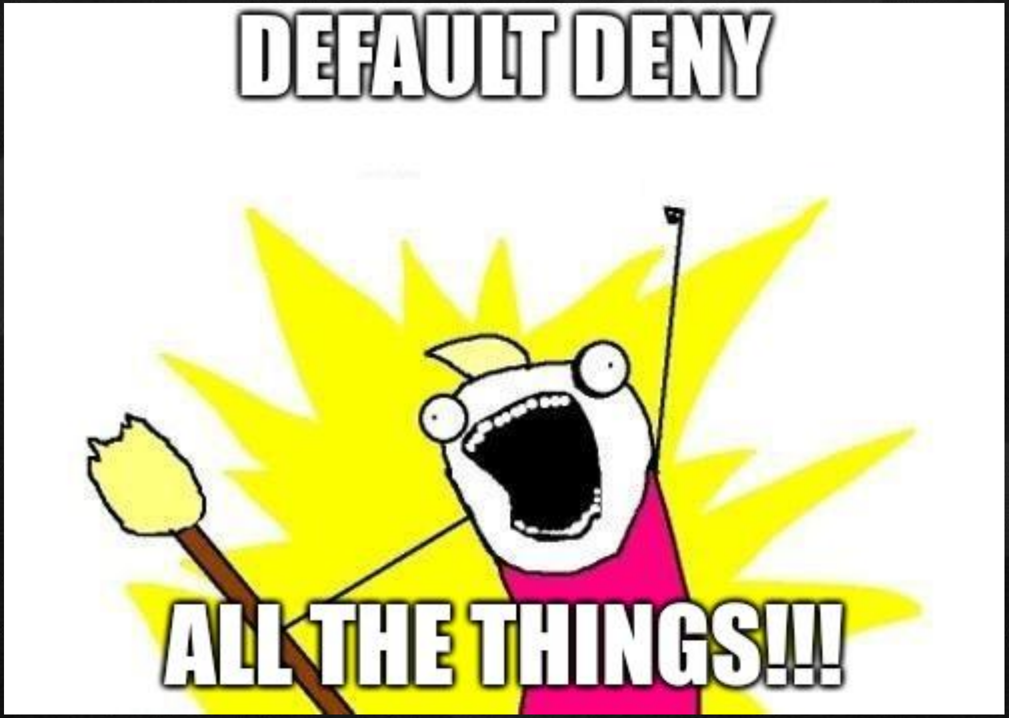
BACnet is a communications protocol for building automation and control networks. It was designed to allow communication of building automation and control systems for applications such as heating, air-conditioning, lighting, and fire detection systems.

EtherNet/IP was introduced in 2001 and is an industrial Ethernet network solution available for manufacturing automation.

The problem – etc...

- *Scanners, like Nmap, masscan, zmap.io have reversed the attack pattern (get the CVE, **then** find the victim)*
- *Domain names: scada.myfactory.co, roomba.family.home*
- *Github code*
- *Numerous ways of authentication & authorizing access; not a lot of standards with developers*
- *Et cetera...*

Intermezzo

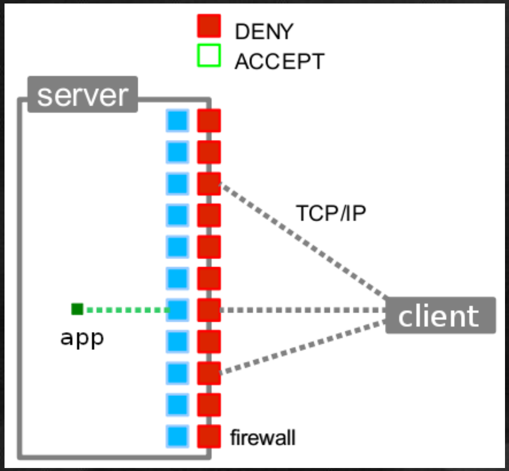


Port knocking - 1

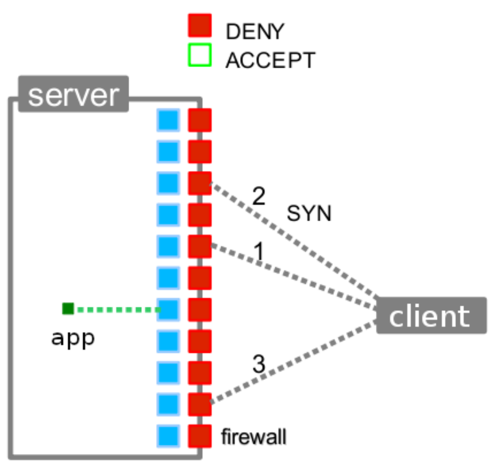
“Shave-and-a-haircut-…-two-cents”

Port knocking - 2

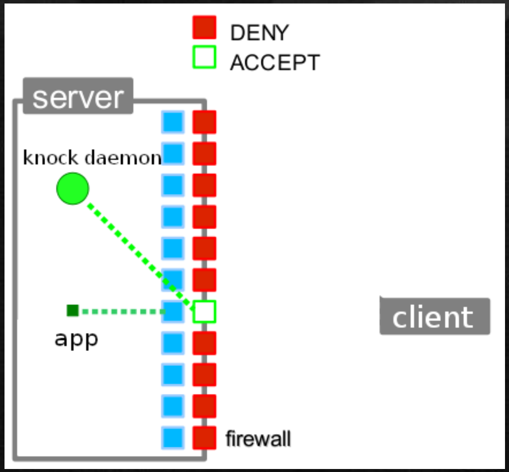
1)



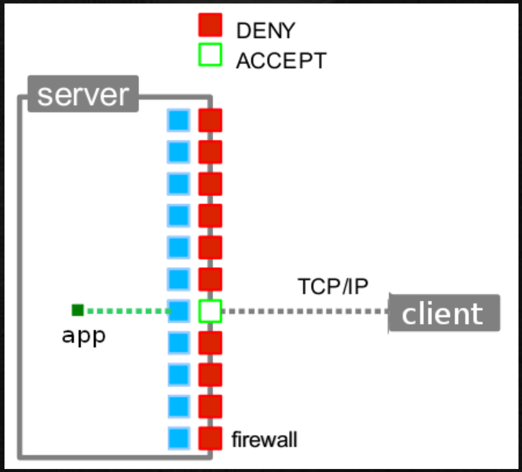
2)



3)



4)



Problem solved!

There might be dragons...

- *Repeatable*
- *Can be observed*
- *No proper authentication*
- *One size fits all*

SPA

Or

Single Packet Authorization

Single Packet Authorization - 1

- *It is not meant to obscure services in the traditional meaning*
- *It is meant to slow down or stop ‘banner harvesting’ and other fingerprinting techniques*
- *If you read carefully, almost all critics discuss running servers… well, guess what… your Roomba should not even **be** a server*
- *It is no silver bullet, but it helps*

Single Packet Authorization - 2

https://github.com/moxie0/knockknock

https://moxie.org/software/knockknock/

- *Encrypted & signed*
- *Prevent replay – Nonce/randomized padding*
- *Less chance of triggering IDS (single SYN, so no ‘scan’)*
- *Tails kern.log*

Single Packet Authorization - 3

https://github.com/mrash/fwknop

https://www.cipherdyne.org/fwknop/docs/fwknop-tutorial.html

- *Encrypted & signed (can use GPG, does not use S/MIME)*
- *Prevent replay – Nonce/randomized padding*
- *Less chance of triggering IDS (single packet, so no ‘scan’)*
- *User differentiation – Alice may knock differently from Bob*
- *Runs over Tor*

Single Packet Authorization - 4

In essence, a SPA packet has:

- Authentication information

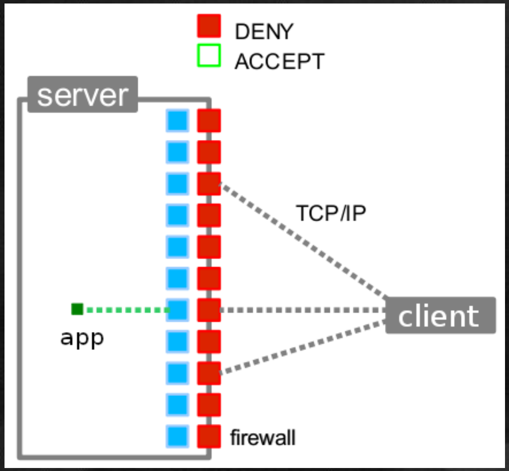
- Origin information

- Service request

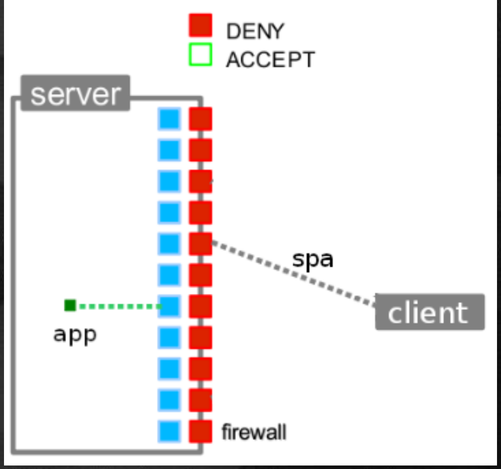
- A nonce/random data

Single Packet Authorization - 5

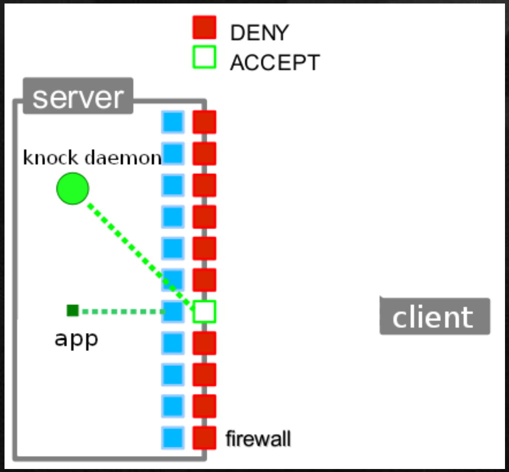
1)



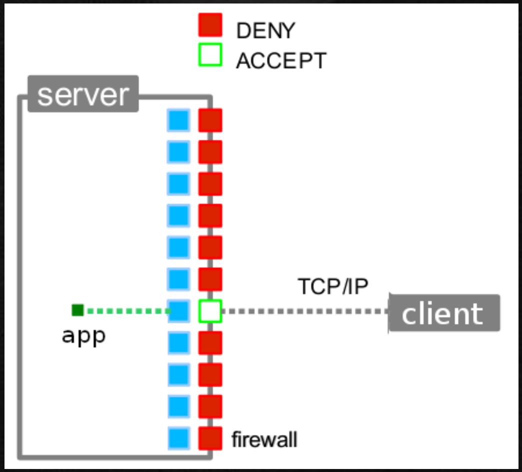
2)



3)

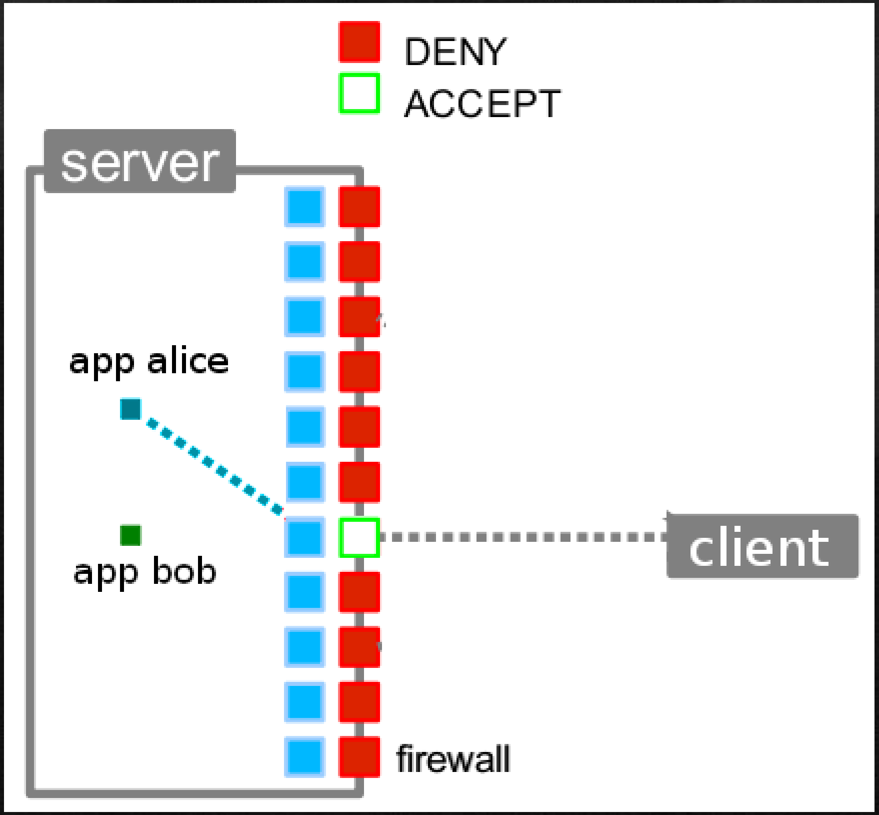


4)



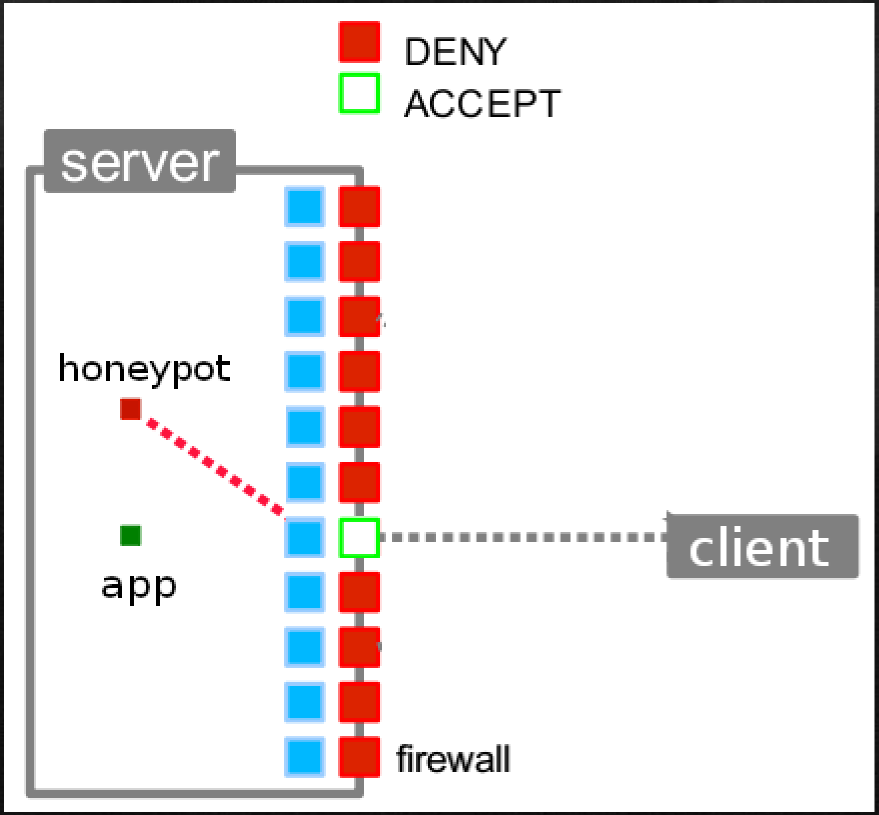
Single Packet Authorization - 6

But there was some mention of user differentiation?

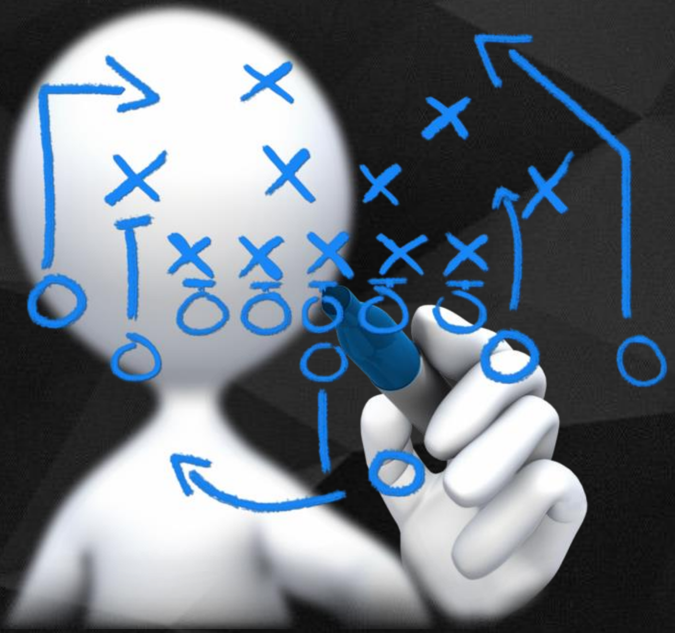


Single Packet Authorization - 7

Since we manipulate iptables, why not...



Game on!



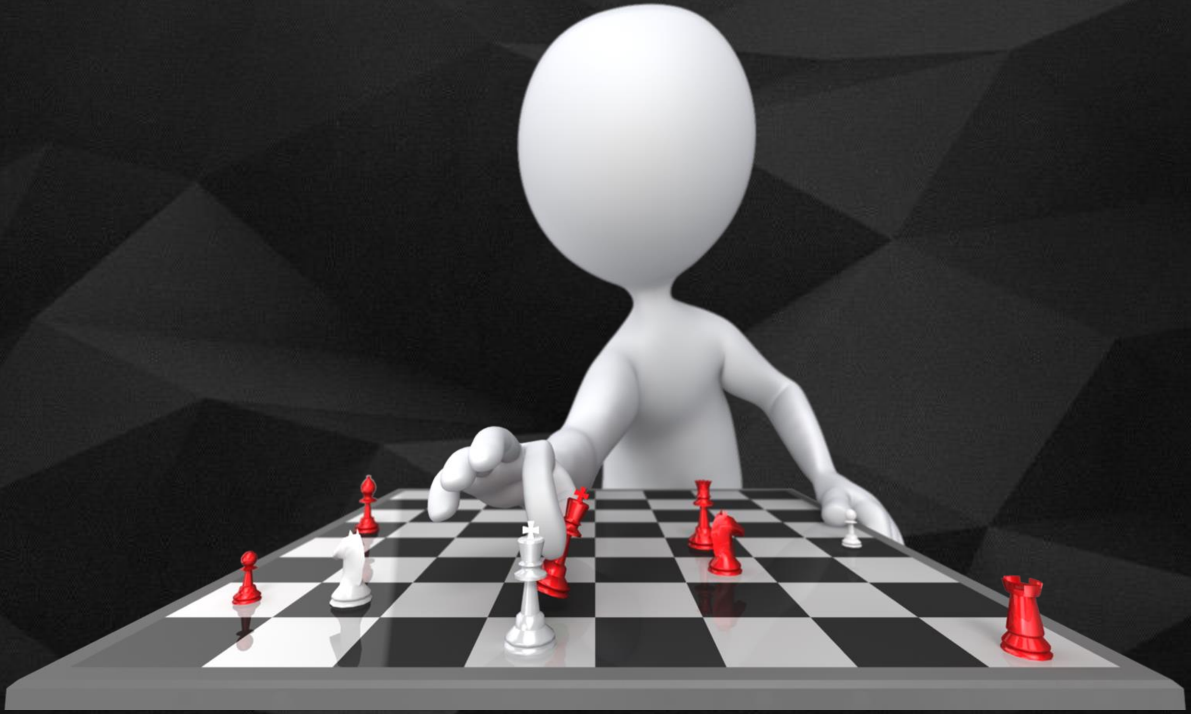
Packet level

- *Give different OS-fingerprint every day*
- *Use tar-pitting tactics*
- *Send unsolicited answers*
- *Play proxy to a random host*

Service level

- *Use standard honeypot software*
- *Make your own (it is fun: https://lets.g0.rs/find/step0001/)*
- *Play proxy (with lots of logging) to a police server*
- *Counterstrike! A tcp connection goes two ways!*

Game over.



Recap

- *Software is insecure*
- *IoT makes a lot of ‘software’ reachable*
- *Productivity is a thing*
- *So is cost*
- *SPA switched on by default can mitigate some errors...*

Questions?