TelSoc
Telecommunications & the Digital Economy
Published on *Telsoc* (https://telsoc.org)

Continents to Islands

Kayne Naughton [1]

Asymmetric Security

AJTDE - Vol 3, No 4 - November 2015 [2]

[3]

☆ 94 [4]

Abstract

Interconnected devices and the true ?internet? cause security challenges to organisations with critical legacy systems. This article discusses a number of legacy issues around Industrial Control Systems and ?untouchable? legacy devices and proposes a number of easy and effective mitigations to the practices that expose them to the world.

Introduction

Ubiquitous interconnectivity of our devices has an amazing effect on society and our ability to respond to disasters. Widespread access to education, health information and even things as simple as weather alerts and fire warnings can save hundreds of lives with relatively little investment.

Unfortunately, although this connectivity is great for people, it has a grim effect on key pieces of our critical infrastructure?many of which are poorly understood relics of a bygone era. I would argue that we are really seeing a true ?internet? now?we are getting a world of true device-to-device interconnectivity rather than the cold war era [IF1] [5] paradigm of segmented, isolated and firewalled networks that provide partial interconnectedness.

Universal Plug and Play, NAT, HTTP tunnelling and other ease-of-use technologies mean that your iPhone-programmable Philips Hue light bulb (Philips nd [6]) can talk to a Latvian university students? networked Quirky Egg Minder (Quirky nd [7]) (a very real example of Internet of Things gone too far).

While these technologies are generally not supported in the workplace, ad-hoc Wi-Fi on mobile phones or unauthorised ADSL services can bridge the gap. As John Gilmore said, ?The Net interprets censorship as damage and routes around it? (Elmer-Dewitt 1993 [8]).

Internet of (Dangerous) Things

As I write this piece there are over 120 Internet- exposed devices in Australia happily chatting via the Modbus industrial control protocol to anyone that would like to have a conversation (Shodan nda [9]).

[10]

Figure 1 ? Concrete batching plant controller, courtesy Shodan.io

Some of these devices control the environment of a data centre or are network controlled power devices, some control the ratios of ingredients used to mix concrete and others make sure industrial safety systems are operating in normal parameters.

Industrial Control Systems (ICS) were developed in a kinder, gentler time, when only people wearing hardhats and overalls could log into them from physically connected luggable computers to adjust a few parameters. Many of them even pre-date the now compulsory blaze orange safety vests seen on industrial sites.

While there is a new generation of secure devices available, the vast majority of still-reliable equipment in the field use naive protocols?they trust their neighbours, are happy to take someone at face value and don?t lock their doors at night.

Do not be fooled into thinking this is a problem for large power and water companies. If you operate a remotely modern office building you will have network connected power (?Uninterruptible Power Supply?, or UPS, is one of the most ironic acronyms of all time), heating, cooling, fire suppression, door control and a slew of other weird odds-and-ends.

While people may laugh at the networked Egg Minder, we have very similar (albeit larger scale) devices in every industrial building in the country. It?s not such a funny idea when the Internet of Things is responsible for the measurements we use to determine food safety.

Real risks

In 2002 Joseph Konopka (or as he called himself, ?Dr. Chaos?) (Williams 2005 [11]) was sentenced to 13 years in prison for conspiracy to commit terrorism. Konopka, a former system Administrator, recruited teenagers on the Internet to help him commit more than 50 acts of vandalism, including causing 28 power outages and setting fire to a sauerkraut factory.

While Konopka used the internet to coordinate his attacks, he relied 0n direct physical means (typically arson) to cause the disruptions.

Bear in mind this was prior to 'social networking? and before a lot of research on ICS was available to anyone with a data plan on their phone. It is easy to imagine what a similarly motivated person or group could do now if they were to shift their digital web defacement goals to a more direct physical facing attack.

Untouchables

While ICS are relatively easy to find and measure due to unique protocols, there is a far more insidious problem on the internet - the ?untouchable? systems.

Many readers will recognise these:

- They tend to be a ?beige box? (from original manufacture or from accumulated dust and sun damage);
- they live under a desk; and
- they have a post-it note saying ?Important 24/7 in use. Do not TURN OFF !!, Call <indecipherable> for info? on them.

Untouchable systems typically run business critical functions (as far as anyone can tell), rely on software that won?t run on anything later than Windows NT and typically are only truly decommissioned during office moves or when they suck enough carpet fluff into their CPU fan that the processor dies and a series of panicked data recovery attempts begins.

As noted with ICS, untouchables tend to be ?designed? without factoring in Internet connectivity; they are generally desktop builds that require sitting at the keyboard to operate. More often than not they have no IT visibility, in terms both of risk oversight and the fact that IT people cover their eyes and mutter to themselves when passing the locations where untouchables reside.

With demands for 24-hour support, measured Key Performance Indicators and increased efficiency, it is quite common for someone to come up with the idea of installing a remote desktop tool such as Virtual Network Computing (VNC) onto these systems. Typically, this will involve having someone poke a hole in the firewall for it, giving a support officer the ability to log in from home and restart a job should an overnight batch FTP transfer fail.

Every time I?ve seen these services they are thought of as ?internal? and very little if any thought is dedicated to choosing a strong password or restricting their access. It?s just a little work-around that ?we?ll get around to fixing later?.

[12]

Figure 2 ? Non-authenticated Carwash control console courtesy Shodan.io (via @yinettesys)

Shodan.io, billing itself as the ?world's first search engine for internet-connected devices? provides a treasure trove of ?untouchable? and accidentally exposed systems (Shodan ndb [13]). I regularly use it when I encounter an unknown device in a security testing engagement to determine how common the device is and what other services it may share. All too often I?ve searched Shodan for a relatively obscure model number and found myself with details of an Internet exposed tape backup library or thousands of remote management consoles.

In late 2014 a website called ?VNC Roulette? appeared in conjunction with the German Chaos Computer Congress (Stevenson 2014 [14]). It used VNC server scan data to connect visitors to an unauthenticated VNC system at random when they visited the page. This project was spun up largely because of the one gigabit per second internet link available at the congress, and was likely inspired by the public but ?non-interactive? disclosures of open VNC systems by Dan Tentler (Tentler 2014 [15]).

Screenshots show people finding themselves (virtually) at the controls of a water pumping facility, alarm systems, an Android mobile phone or the audio visual controls for a meeting room. Many delegates took the legally questionable effort of securing these systems for their owners.

Although the site has been taken down by the operators, it is worth noting that a vaguely motivated party with basic computer skills could reproduce this tool in a fully interactive way by watching a couple of Youtube videos. High bandwidth, cheap server hosting is provided by cloud vendors, typically by the hour, allowing this to be done in hours for tens of dollars.

Boxing or Judo?

Security is an ever-evolving struggle between our attempts to make a system difficult to breach while still being usable, efficient and cost effective. As much as it pains security teams, the convenience of internet (or commercial network) connected control terminals far outstrips the security demands of isolating these devices. In places where interconnectivity is prohibited, there is a tendency for team members to find inventive ways around the larger IT policy in order to meet the demands of their own work. In many cases, this will involve a sneaky 3G dongle here or a rogue ADSL link there.

Security and networking teams really need to work with their businesses and go where the organisation is heading. As much as you would like to ban web browsing in the workplace or prohibit Bring Your Own Device, outside of restricted government areas this tends not to be a viable option.

Implementing ?bastion? hosts to control access to sensitive environments helps secure the critical systems, isolates them from the general desktop fleet and lowers support costs by reducing the number of systems that need custom software installed to manage devices.

Lack of any policy is worse than a non-workable policy and you will find little clusters of cloud services springing up, from teams with private Dropbox clusters replacing your painful per-share provisioning process through to your enterprise source-code on a free Github account because your Subversion repository isn?t as friendly to use.

Work with your users, shift their direction and use their momentum like a judoka rather than trying to beat them down like a boxer.

Fixing the mess

Unfortunately, most security and network design takes places at a project level, where a system is considered as a whole, with the inputs and outputs mapped and the importance and functions of various systems entered into a matrix. We rarely revisit these assumptions or the moving targets they were made around.

From my perspective there are four key strategies to deal with the obvious disasters lurking around the corner with increased interconnectedness:

1. Put controls into the purchasing and provisioning processes at your organisation ? for all

purchases, implement non-technically-worded governance processes to ensure that passwords are chosen and basic security controls/access restrictions are in place. Know how old systems are and plan for their periodic replacement. IT teams can be easy to ignore but, much like in cybercrime, we can ?follow the money? to identify unsupported computer or device purchases. Likewise, ADSL links on the corporate phone plan should trigger an IT ticket to ensure that they are authorised and adequately controlled.

2. Revisit what you have ? network scans are cheap and easy. Blow the dust off the logs from your perimeter Intrusion Detection System and you?ll see that hundreds of aspiring computer criminals around the world can manage to scan your environment so surely you can too. We tend to look at IT infrastructure and networks through the keyhole of projects and risk management. A quick periodic perimeter scan and a comparison against previous results will help you find unmanaged systems, accidentally exposed services or stealth changes made outside of change control.
3. Engage collaboratively ? as noted above, a ban will give people a reason to route around you. If you are applying a good risk management approach, you will need to identify where you can compromise and make a ?better than nothing? choice in order to save up your political capital for when you really must put your foot down. IT and networking in modern businesses are advisors, not wardens. As I heard Laura Bell (?Stilgherrian? 2015 [16]) say earlier this year: 'We need to create an environment where it's actually safe for us to go: "This feels funny. I do not like this. Hello, people, look at this. Does this look strange to you?" '.
4. Build a security culture?Talk to staff members regularly about security and why it is important, especially in the context of your business. Posters or yearly online training courses do not change the way people think about things; they need regular, light touch points.

References

Elmer-Dewitt, P. 1993. "First Nation in Cyberspace".*Time*, December 6, 1993.

Philips. nd. Hue Developer Program. Available at: http://www.developers.meethue.com/documentation/getting-started [17].

Quirky. nd. '" EggminderSmart Egg Tray". Available at:https://www.quirky.com/invent/243958 [18]. (n.d.).

Shodan. nda. Available at: https://www.shodan.io/search?query=port%3A502+country%3Aau [19].

Shodan. ndb. Available at: https://shodan.io [20]. (n.d.).

Stevenson, K. 2014. Available at: https://medium.com/@kylestev/open-season-on-vnc-servers-around-the-world-4b89a0f8d992#.upg2z0hyb [21].

?Stilgherrian?. 2015. "Spearphishing and how to stop it: Some lessons from AusCERT". Retrieved from ZDnet: http://www.zdnet.com/article/spearphishing-and-how-to-stop-it-some-lessons-from-auscert/ [22]

Tentler, D. 2014. "Atenlabs ? Scanning the whole internet".http://atenlabs.com/blog/scanning-the-whole-internet/ [23] . (n.d.).

Williams, J. 2005. 'SUPERVILLAIN' GETS HIS ARSON SENTENCE TOSSED 'DR. CHAOS' WINS AN APPEAL ARGUING THAT A FEDERAL STATUTE SHOULDN'T APPLY TO ARSON CRIMES. *Madison*, Jun 1,2005.

[IF1] [24]Are we definitely referring here to the 70s/80s?

Copyright notice:

Cite this article as:

Kayne Naughton. 2015. *Continents to Islands*. ajtde, Vol 3, No 4, Article 35. http://doi.org/10.18080/ajtde.v3n4.35 [26]. Published by Telecommunications Association Inc. ABN 34 732 327 053. https://telsoc.org [27]

Industrial Control Systems [28]

Critical infrastructure [29]

Legacy systems [30]

Industry case study [31]

Legacy systems [30]

Source URL:https://telsoc.org/journal/ajtde-v3-n4/a35

Links

[1] https://telsoc.org/journal/author/kayne-naughton [2] https://telsoc.org/journal/ajtde-v3-n4 [3] https://www.addtoany.com/share#url=https%3A%2F%2Ftelsoc.org%2Fjournal%2Fajtde-v3-n4%2Fa35&amp;title=Continents%20to%20Islands [4] https://telsoc.org/printpdf/1155?rate=mvu9c_Yi7J3pF8LPf2F9OG4VxGswcNXiJyQAziXYmAU [5] https://telsoc.org/journal/ajtde-v3-n4/a35#_msocom_1 [6] https://telsoc.org/journal/ajtde-v3-n4/a35#PHILIPS_ND [7] https://telsoc.org/journal/ajtde-v3-n4/a35#quirky_nd [8] https://telsoc.org/journal/ajtde-v3-n4/a35#ELMER_1993 [9] https://telsoc.org/journal/ajtde-v3-n4/a35#shodan_nda [10] https://telsoc.org/sites/default/files/images/tja/35_figure_1.jpg [11] https://telsoc.org/journal/ajtde-v3-n4/a35#WILLIAMS_2005 [12] https://telsoc.org/sites/default/files/images/tja/35_figure_2.jpg [13] https://telsoc.org/journal/ajtde-v3-n4/a35#shodan_ndB [14] https://telsoc.org/journal/ajtde-v3-n4/a35#STEVENSON_2014 [15] https://telsoc.org/journal/ajtde-v3-n4/a35#TENTLER_2014 [16] https://telsoc.org/journal/ajtde-v3-n4/a35#Stilgherrian_2015 [17] http://www.developers.meethue.com/documentation/getting-started [18] https://www.quirky.com/invent/243958 [19] https://www.shodan.io/search?query=port%3A502+country%3Aau [20] https://shodan.io/ [21] https://medium.com/@kylestev/open-season-on-vnc-servers-around-the-world-4b89a0f8d992%23.upg2z0hyb [22] http://www.zdnet.com/article/spearphishing-and-how-to-stop-it-some-lessons-from-auscert/ [23] http://atenlabs.com/blog/scanning-the-whole-internet/ [24] https://telsoc.org/journal/ajtde-v3-n4/a35#_msoanchor_1 [25] https://telsoc.org/copyright [26] http://doi.org/10.18080/ajtde.v3n4.35 [27] https://telsoc.org [28] https://telsoc.org/topics/industrial-control-systems [29] https://telsoc.org/topics/critical-infrastructure [30] https://telsoc.org/topics/legacy-systems [31] https://telsoc.org/topics/industry-case-study