“Security” its not just adding an S

“We need to be Secure”

This is the buzzword exclamation echoing around boardrooms right now. If we delve a little deeper and ask “why?” an honest exec (obviously after the requisite superiority posturing (almost as tiresome as the technical “boring” answer), will conclude “if we don’t we can get fined huge amounts of money. This sets in motion our friend, complete “normal” behavior. The least competent, and most powerful, out of fear, react without understanding. They kneejerk to their “trusted” self appointed advisor (probably some bloke they met at the golf club, who “has a business” doing that sort of thing. The golfclub bar fly means they saw an opportunity, hired some “clever” but cheap inexperienced grads, and out of the goodness of their heart decided to give these clever people a “leg up” (and make a load of money for themselves into the bargain.

If the exec had a strong understanding of this “boring” (and yes it is very boring) matter, they would find that its just “business”. We succeed in business (or not) by taking quantified, calculated risks. We start with a risk assessment. In “security” these fall into two categories (like usual). 1. Regulatory consequence, and 2. Consequences of well-intended incompetence! The headline “bad actors” is actually a very small risk in most places. I go so far as to suggest that most people in planet earth are more concerned with just getting through today, like they did yesterday. “Bad” people are such a vanishing minority, that devoting vast resources to their hypothetical (mainly) existence feels a little paranoid. However, whilst I hold this idea up to suitable ridicule, in a communications network, we potentially mobilize this tiny minority.

“Oh come on” (sigh puff) “get to the point, you haven’t said anything”

This is the “normal” reaction of an exec. To be fair, its not completely unfounded. OK, traditionally we would stop a bad person from coming into the golf club, by imposing a dress code. Not having a suit was a minor inconvenience for the slightly motivated con artist. This eventually failed, now, suspicion grows with expensive tailoring. If they have a good suit, but you don’t know who they are, they probably obtained the funds for the suit, the Rolex, and the Porsche through “unfair” or easier ways, or in their view “efficient”. So, we respond – lets get some ID… I know, a club tie! That will fool everyone! Oh and we will make the supplier exclusive.

This is why “Authentication” is necessary in a security posture. Who are we listening to? Can they give evidence of their identity? Should we share the keys to do stuff with them? If it turns out they are bad, how do we exclude them?

We focus heavily on Encryption – this is understandable. The romanticism of oak panneled lectures with a lecturer scribbling franticly on a wall of rotating blackboards is emotionally attractive. The human metric of “hard graft” is compelling, but flawed! The paradox of “corporate” where “plagiarism is bad” (only if you get caught) but “hard work” is disproportionately rewarded “look busy the boss is coming” sadly still works. I’ve met many people who “work hard” who achieve nothing, or indeed make things move backwards. This seems to me to be the opposite of the intent.

Contrast this with “every one else is doing this” which is exactly why you need to be doing something different.

Why this is dangerous

HTTPS, LDAPS etc… must be secure, the acronym says so! Well, LDAPS is less secure than LDAP with TLS (a “boring” detail). “so S means it isn’t secure, how am I supposed to tell?” well, I’m terribly sorry to tell you this Mr exec, but the law makes it incumbent on you to actually know! Better do some of that “hard work” you tell everyone else you admire! “ah well I’ve got lots of money, I’ll hire a consultant, and they can take the blame for me – back to my yacht, and you pleb, get out!” all I’ll say to that is that I “really wouldn’t want to be your lawyer”.

Another problem doom sayer without a solution

Au contraire. First lets examine the risk. The greatest being a fine from legislation that is heavy handed. It is likely that this is a wakeup call. It allows the government to flag the “real problem” and in a paternalistic way encourage people to be more serious. Modern legislation seems to have grown sick of “outsourcing blame”. This feels positive to me. It is actually relatively easy to achieve, and the more you spend the less likely you are to succeed. That got your attention!

Cheap can mean good, and free can be better!

I love ACME – this is Automatic Certificate Management Environment. It is open-source, and one can get a free certificate from letsencrypt.org. “ACME that’s roadrunner, it’ll explode”, oh dear, its not really my fault you skipped classics classes. Don’t you think the company called “Looney Tunes” was the one making the joke? Whilst because networking is inherently boring, it is not debated or conceived by stupid people! Letsencrypt.org is the ISRG Internet Security Research Group. It gives away certificates, because they are just numbers. They are absolutely serious. These are good people, doing good things. They get their funding from serious people, not by pulling a fast one and spending money telling you that if you pay me, you’ll look clever (which is a good thing – their website isn’t pretty!)

A fool and their money are easily parted

Solution – don’t be a fool. We’ve established that the ACME (Zenith not roadrunner) of certificates is free! You just need to register a domain, then let your local open source ACME bot in, it will give you the keys and certs, and automatically rotate them every 60 or 90 days. Given that an x509 certificate would take thousands of years on the worlds fastest computer to “crack” through brute force, changing every 60 days is a pragmatic security measure, and it didn’t cost anything!

Ok infrastructure. No it isn’t free, but because we are focusing at securing the top of the network stack, and therefore not actually that worried about the physical cables at the bottom, or the stuff in the middle, assuming we can put only encrypted messages into the network, then a “hacker” can go enjoy the next millennium decoding some soulless corporate theory (which we know will be significantly revised before anyone actually takes meaningful action). The reason why this works is because “hackers” are lazy, if they see “work” they look elsewhere. Just making it unattractive (the date from hell) makes them go away.

It's a simple choice – do we employ our middle ages mentality, we take our beautiful, high maintenance expensive "princess" box, and lock it in a dungeon, where only the special people can see it. This will have been supplied by a person in a nice suit, with expensive shoes, driving a premium motor vehicle (probably German). Or do we take a helpful, reasonably priced work horse of a piece of software (also probably German ironically) and use that, and then find a real princess?

The middle aged/s matchmaker

OK so I'm now going to "sell" you something. Don't worry, its actually free, well, its free, and works. If you want to be responsible, and hire help, not shift blame, then you can pay the developers directly, but it merely changes you from being an opportunist, so a functioning member of society.

1. Proxmox – this is built on Debian 12 (or 13) this is the open source Linux kernel in action. You don't need to pay for it, it's a good idea to pay for access to their curated and tested update repositories. This replaces VMWare – which is a fine piece of software, but now with its new owners (Broadcom) it is charging like a wounded bull!
2. OPNsense An opensource based firewall. Again, it can be used for free, and again the "business edition" for a reasonable fee supplies you with tested and patched repositories.
3. Ubuntu. This is a "friendly" linux environment. Again, use as many boxes as you like, for free. If you want to buy Ubuntu pro, then Canonical (the maintainers) will help you out, and guarantee their Repositories (which include most of the things you need. This centralises having expert support for things like LDAP and Guacamole (for remote desktop viewing – the best way to stop a USB key social engineering attack). Ubuntu pro looks expensive, until you realise what it is doing!
4. LAM pro – Roland Gruber's "friendly" way to manage LDAP trees. He charges for the pro version, but it is available in a free version, and he isn't stopping you from learning LDIF if you don't want to pay him. However, it takes some pain out, and he is very pleasant, and very smart. You could do far worse than looking at this.

This 4 point plan is all you need to set up a system that stops using passwords, and starts using cryptographic keys for authentication. It costs very little (and is free if you want to do it yourself). We have a financially palatable, and defensible stack. Now all we need is for equipment manufacturers to stop getting in the way of security! I like pretty looking "Princess" boxes as much as any other gear geek, but like the Austin Princess, they might get a bit "rusty" and not age well!