The Certificate Fashion Show and the Fashion Police

Introduction

In the fashion world style matters and designers put their wares on display for the critics to comment. Fashion is a highly subjective thing but somehow many of us know what works and doesn't even if it boils down to personal tastes. This allows a wide range styles that can accommodate a wide range of uses. So why a discussion of fashion when it comes to cybersecurity and Eidola. Well, it seems that style matters greatly when it comes to the use of digital certificates. Cross certain style lines and its time to call the certificate fashion police. And why not have a little fun with what for many can be a very dry topic. Rodney Thayer of Smithee Solutions and I have been working together on digital certificate related topics for more than 15 years (Rodney even longer). I am often referred to as the policy diva and Rodney as the standards enforcer who can code crypto with his bare hands, partners in fighting certificate misuse. It makes for a pretty cool team and we have collaborated to bring the Eidola product to market. This post also serves as Eidola Application Note #4. Hopefully these examples provide a fun way to get your certificate wardrobe in order.

Making Your Own

My mother was a seamstress and I grew up when clothing patterns and the whir of the sewing machine always resulted in something that was not only cost effective but stylish as well. This was a common skill set among many folks and often taught at an early age and learned over time. There are few barriers to trying to put together a piece of clothing; a pattern (really important) material, scissors, needle, thread, buttons, zippers and some sense of design and you are good to go. That being said do-it-yourself (DIY) is not something that happens overnight in this case and learning a craft takes time. OK if you know what you are doing but be careful with those things where you take on DIY.

The same thing is true with security and in particular digital certificates. It is relatively easy to get a certificate issued using the Certificate Authority (CA) built into server operating systems (e.g. Windows®, RedHat, etc.) and plenty of third party CA's. However, it takes a while to understand the different aspects and whether the pattern matches the use; whether it is the certificate policy, registration and workflow, the cryptography involved (of which there is quite a bit including dual key authentication, encryption, signatures, and hashing), validation and the balance of the public key infrastructure. And the world is not static. More recently things such as certificate transparency[1], considerations for post-quantum crypto[2] and ever widening needs, in particular for the Internet of Things (IoT). In all these cases style cannot be separated from substance.

Taking the crypto example of a need to understand details, often in Elliptical Curve Cryptography (ECC) there is a misunderstanding of what is specified and disagreements among researchers about their security.[3] There are different standards that are in play. There are tradeoffs and differing opinions. For example, P256 has multiple versions and opinions differ. This makes this a bit of the wild west and very hard for those trying to come up with their own designs, definitely not an area where you want to DIY.

Another example of a DIY equivalent is the use of self-signed certificate. While it was really OK to wear the homemade stuff, you wouldn't really offer those clothes up to others (unless they were younger siblings). In the case of DYI you control the input and you know what you need, as soon as this branches out the use case tends to fall apart. What was a bespoke thing with a very tight feedback loop (you know you very well) becomes a very bad "retail" strategy where your tastes and material are foist on 3rd parties.

Details matter in the fashion world and with certificates. We have found in many cases issues with crypto, particularly around how cipher suites get implemented, as above with the math (e.g. curve points) and this is particularly relevant with constrained computing devices that frequent the security world and the internet of things. And in many cases the DYI is then passed along the supply chain from vendor to integrator to end-user further conflagrating the issues around trust for a relying party. Unfortunately, this is not as easy to recognize as three legs in a pair of pants, and not everyone has at their disposal certificate fashion police or the technical automation tools to recognize these design and implementation failures.

Managing Your Wardrobe

We all understand appropriate dress. While the ripped jeans may be cool, they probably are not what you would wear to a Board of Directors meeting. Not all occasions require black tie but, in some circumstances, it was likely made clear in the invitation. In other cases, its best to lose the tie and go with "business casual". And styles change, children grow to adults and believe it or not bodies change over time. All of which means that a wardrobe needs to be managed, even if you have standard uniform you likely don't wear it to sleep. Same holds true for digital certificates, style and substance need to fit purpose.

Not all certificates are created equal and the requirements are different depending on what you are doing, e.g. client authentication, email, or transport layer security. Besides uses, environments differ as well. Federated environments represent particular challenges as do enterprise use cases running across global infrastructure particularly in the age of everything-as-a-service and substantial amounts of information technology (IT) running off premises. The previous comments about self-signed certificates apply here, so don't be surprised if you get reminded of the dress code at the front door. Browsers can be pretty picky these days and for good reason.[4] It is really not the case that one size fits all so be

[1] https://tools.ietf.org/html/rfc6962

[2] https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

[3] https://safecurves.cr.yp.to/

[4] https://cabforum.org/

prepared to manage a mix of certificates. And even in the case of uniforms they do wear out with time so expiration and reissuance are part and parcel of certificate management. And be careful about just ordering the same thing, it probably makes sense to go through the some if not all aspects of registration, just like it might make sense to check your measurements.

And it goes without saying that key management is part and parcel of any successful certificate deployment. And just like managing your wardrobe you do want to make sure that you manage your keys. Even the occasional visit to the dry cleaner or doing a load of laundry maximizes the long-term benefits of that wardrobe. And while you can't clean a certificate make sure they haven't worn out. Which is why very long-lived certificates should be used only when appropriate.

Knock-Offs

Counterfeits impact the fashion world as they do other industries. Just because something has a label on it from a high-end manufacturer doesn't guarantee that its authentic. And some copies can be very good and require an expert to discern the differences. If other cases it can be obvious from pricing and/or from the look and feel. The seller can also be a good indicator of whether or not you are getting the genuine article. The same thing applies in the digital certificate world.

Digital signatures do a lot of the work in helping to determine whether or not a certificate is from a trusted source. The signature can be checked for validity, its issuer can be further examined as to whether or not it is trusted including whether or not the issuer's certificate has expired. The object identifier (OID) is also a useful and often underutilized tool here as well. OID's map to uses and are effectively a dress code. Wrong OID and you are showing up at the wrong party even if you have an invite from the party's host, as it may not be the only gig they are throwing. There are also some cases where you need to stay on top of what is happening with the issuer. As an example, when DigiNotar[5] got hacked, and a private key compromised it became impossible to tell the difference between a real and fake certificate other than a knowledge of the individual certificates. All of which means that you need to establish a trusted supply chain that runs from issuer to end-use. In many cases the certificate that is being presented is at the end of a chain, often there are intermediate certificate authorities and above that at some point a root. All of these need to work together. In the same way that clothiers depend on their fabric, their production and even marketing teams, so to do certificate consumers depend on the certificate supply chain and it needs to be trusted and authentic all the way through.

Don't Get Too Fancy

While you may see some wild stuff on the runway (e.g. the above photo), some styles should be left to the fashion pros. And just because you can get fancy doesn't mean that it addresses down to earth requirements of everyday use. It all depends on your customers and audience.

Again, the same applies to digital certificates. This means that depending on the use case it is best to stick to something in the middle of the bell curve. Too weak a set of keys for a certificate and it can be easily compromised. Too strong a set and the processing load can be onerous, particularly for constrained devices. In some cases, the design guidelines are barely there (a good example would be international passports where there is a very wide range of certificate cryptography in use). As pointed out earlier there exists a fair amount of confusion around ECC and here it is harder to know what the

[5] https://www.wired.com/2011/09/diginotar-bankruptcy/

fashion neutral style choice is, but it is worth investigating. My default would have been P256 but even that seems to be called into question. Things get hard when even NIST standards bring out the certificate fashion police.

Wardrobe Malfunctions

The examples in the fashion world run the gamut from the Super Bowl, to pants riding too low on the big person to the quainter slip showing. In any case clothing and digital certificates are things that are by design made to be seen in public, ergo the name Public Key Infrastructure and public key cryptography. This also means that bad style decision or malfunctions in use are there for all who care to see. This in general is a good thing, and the reason why a green lock for a website and transport layer security (TLS) connection signifies trust and also why most browsers today get pretty cranky when confronted with a bad certificate. And while not all of the IoT or physical security world have signaling around certificate and crypto status the tools exist to make this available for even the layperson to determine whether or not the emperor is actually clothed. In a world in which being able to function properly on a network is a quid pro quo for any security or other network-based product; run afoul of the wardrobe malfunction and the result will definitely be a reputation hit from which it will take time to recover.

One Size Fits All

Nice in concept but very hard to accomplish in reality. Most of us are different and so things need to fit and be fit for purpose. Unfortunately, many certificate wardrobes contain outfits that do not accomplish these goals. One example is the wild card certificate, typically something like *.your-domain.com. Use of wild cards makes things easy since one size fits all, but really how many of us are the same size and even in your organization is it really the case where all of the certificate use cases adhere to the same policy; web sites, client authentication, logical devices, IoT, email, encryption, etc. Other examples simply are mis-use of certificates where the certificate policy (CP) does not meet the use case. The aforementioned object identifier (OID) is a basic alignment point.

Disguises and Cross-Dressing

OK so maybe it is fun every once and a while to confuse people with what you wear. This takes the idea of pushing your expected style envelope one step further. Most of us dress in a way to look at good as possible and to be recognized for it, or at least to be dressed consistently in the context of the occasion. The same thing is true with digital certificates. Certificates, as mentioned, are meant to be public facing and as a result contain information about companies and the purpose of the certificates. They are not meant to cause identity confusion. A sure way to fail any certificate check is for there to be a mismatch between the Distinguished Name (DN) or Subject and the actual web site or manufacturer of a device. Even in the case where certificates are acquired through trusted third parties these things need to line up.

Conclusion

The role of digital certificates is increasingly important. And while not covered here much of what is being discussed applies to the use of other kinds of tokens such a JSON web tokens, or the use of public and private keys with distributed ledgers. But those are a whole different manner of outfit. In the mean time start building your certificate fashion plate with the basics, get a few things off-the-shelf from trusted brands and learn how to take care of those items before you jump on to the fashion runway.