Before I start I have a difficult announcement to make. I knowthis will, without a doubt deeply, upset all of you, but I am sorry, I must.

2 and a half years ago I discovered greatness, and I was immediately hooked. But like so many partnerships through history it wasn't to be. And so I regret to inform you that this, as you may have glimpsed, was made in ***Google Slides*** *and not in Figma. As will every presentation I do from nowon.*

NowI am not done with Figma completely. It's still great. Kelly you should totally use it. But its a lot of effort using it to make a presentation that is only going to be seen once.

But as you may be able to tell, ***I*** *do like putting on a show. So, if you'll join me, lets send Figma off to the next life with a round of applause.*

Goodbye, my friend. wipes non-existent tear* *

Oh and by the way the notes for this presentation can be found alongside the rest of my notes on my website so don't worry about typing.

So, now that I've wasted 2 minutes of everyone's time, Attack vectors.

Now all of these surround the idea of networks, so let's start with general issues that arise around internet connection.

The main one is different types of Man In the Middle Attacks, like ARP spoofing or compromised network equipment. The end result, if through pretending to be the network's router or otherwise, is the ability to intercept and alter network traffic.

If DNS poisoning is used along with some certificate forgery, then requests to a legit site get data from a fake provider instead of the real one. Users could unknowingly type their password into what they think is the real site but is in fact a login stealer.

So how can this be fixed? Well using known secure DNS resolvers like Cloudflare or Quad9 is a start - this stops DNS poisoning for the most part.

Other good ideas include using HSTS to avoid forging of certificates, making sure end-to-end TLS is used. Segmenting the network into VLANs will also help to avoid other MITM attack exploits as security is mandated and any unusual traffic can be sealed off.

The other large vulnerability is open ports. A port on a host can accept any network connection so long if there is a service listening on that port - generally this is a set port for a given protocol.

This however, is an attack surface. *Some* protocols or applications may be fine, but even so, if this service is vulnerable for any reason, like if it is even slightly misconfigured, then it is a risk too.

Open ports are an attack vector because these services can be exploited by attackers, which could result in footholds like remote code execution. They can also be used for lateral movement - allowing an attacker already in one part of the systems to move throughout the network.

The solution in an immediate sense is to close these unnecessary open ports. This seems obvious but can be finnicky as sometimes services have to be reviewed on a case by base basis. An additional layer of protection is a firewall and have it allow only required ports and addresses - and deny everything else. Another good point is not

to expose admin services to the internet - require a trusted VPN or some other form of protection.

Now let's look at Wi-Fi specifically. **A** very common attack is the Evil Twin attack. This is where a Wireless Access Point is created matching the SSID of a legitimate network. This it is hard for users to detect, as the names will appear identical. This is especially effective on unencrypted or poorly configured Access Points. In cases of areas with public Wi-Fi, some phones will connect to open Wi-Fi automatically which could pose a risk to them.

Once users are on the Evil Twin, their data may be harvested - or the corporate Wi-Fi sign in page may be duplicated. One user unaware of what is happening logging on is all it takes for attackers to get a foot in the door.

Defenses are more difficult because some of this is down to users. For most users, a VPN in use on any public Wi-Fi is enough, perhaps making sure auto-connect is off too. For organizations, using WPA2 or WPA3-Enterprise encryption and a Wireless Intrusion Detection System would be good mitigations.

Now let's look at Bluetooth. **Devices** with Bluetooth can be spoofed and paired without consent. Unlike Wi-Fi, attacks usually require physical proximity, but that still makes Bluetooth a risk for offices and public spaces. While Bluetooth does have encryption and security, older versions use very vulnerable connections and even more modern secure connections do not eliminate risk.

This impersonation or pairing can be used to access services or transfer files from and to nearby devices. This not only is a malware risk but a data security risk. Legacy connections may be intercepted

and the data harvested. Smart devices could have commands or events triggered, causing disruption.

Solutions involve a varied number of things, including segmenting Bluetooth devices from other devices on network, maintaining an inventory of Bluetooth enabled devices and logging pairing events in the organization's SIEM.

Now, we can also consider the prospect of the attacker already being inside of the network. **In** this case, some of the solutions provided earlier are moot. The attacker can attempt to access key infrastructure without the worries of a firewall for example.

This key infrastructure could be file servers containing documents and potentially confidential information. It could also be similarly important communications stored on a mail server or could be a web server which could provide the organization's services.

Solutions in this case are more general internal security. Isolating the key infrastructure and enforcing access control for it is a good start. That ties into the next one which is to follow the principal of least privilege. Finally, anomalies and unusual access patterns should be logged in a SIEM.