Disklabs®
THE DATA EXPERTS

White Paper

FARADAY SHIELDING

Helping to secure the mobile workforce

Does your mobile workforce use laptops and mobile phones?

Think about the information accessible from these devices and how it could damage your organisation if it got into the wrong hands.

It is not possible for IT Managers to guarantee that security discipline is always maintained by the mobile workforce when away from a principal site.

This is presenting a growing risk to government and business organisations that deploy a mobile workforce.

The simple substitution of a conventional laptop bag with a faraday shield variant will help to significantly reduce the risk of malicious attacks and unauthorized access to data via wireless connectivity.

Contents:

MAKING THE MOBILE WORKFORCE MORE SECURE

We have entered the age where mobile devices provide all the tools and technology to enable employees to work away from an organisations principal location. Workplace flexibility is increasing year on year with significant benefits in efficiency and convenience however this change in culture is also introducing new and growing risk to networks and data.

Not many of us would leave a device unattended or unlocked in an unsecure environment, however physically carrying or using a computer or phone is no guarantee that the device is secure and not at risk from unauthorised intrusion.

Most employees will understand the importance of keeping the organisations data secure. Strict but workable IT policies will gain the buy in from employees and ensure they are more open to approaching the organisation with security concerns.

So how do we ensure that the mobile workforce buy into and support the security requirements of the organisation? The best way is the supply of appropriate training and equipment relevant to their mobile working environment. A policy that has empathy with the challenges of the person working in the field is more likely to be accepted. That will still leave a risk that wireless security policy may not always be adhered to. Although not a panacea for all security issues a faraday shield for the digital devices used by mobile workforce is an important addition to the IT Managers tool box of preventive measures employed to keep an organisations data safe.

This whitepaper will highlight the risk of data theft from any device that has the potential to connect to a wireless data network and how new bag and sleeve designs that incorporate shielding will be beneficial in significantly reducing this risk.

WIRELESS NETWORK SECURITY RISKS

Restricting the use of all third-party Wi-Fi networks is usually impracticable and defeats many of the benefits of the mobile workforce so IT Managers will mitigate this risk through training of staff on the type of networks that should be used. Additional security protocols required during log in (e.g. VPN , two factor authentication and encryption) are essential in preventing attacks however a faraday shield offers the first line of defence.

Simple precautions on third party networks such as avoiding sites that do not use passwords, ask you to re-enter your password or have invalid security certificates is simple for the mobile workforce to assess and follow.

The faraday shield will not prevent the risks to the device when Wi-Fi or Bluetooth is enabled by the user however it will protect the device from malicious attack assuming it is not switched off or put into 'airplane mode' after use.

The following scenario is just one way that your computer could be at risk and shows how an isolated device is protected.

One common way that hackers will gain entry to a device is by use of what is commonly called 'the evil twin'. This is a fraudulent Wi-Fi access point that appears to be legitimate. A good example would be an airport lounge network and although the hacker may struggle to override the legitimate Wi-Fi security protocols in the lounge itself there would be nothing to stop a hacker setting up elsewhere in the airport or even in the aircraft. A targeted computer could still be at risk if it was in standby mode and not powered down as it may recognize and reconnect to what it thinks is this network.

Phones can be even more susceptible and will automatically connect to what it thinks are trusted Wi-Fi networks. The security protocol of many phone apps is poor and they will leave a back door into the device.

This is a typical scenario where the faraday shield may prevent such an attack because even with device in standby and the Wi-Fi left on, the bag would isolate the device from wireless connectivity.

WIRELESS NETWORK SECURITY RISKS Continued;

Also, if Wi-Fi is left on whilst passing through a transportation hub the firewalls and encryption may prevent access to a computer however there is still useful data that can be gained from capturing an IP address, at a specific time and location (pattern of life surveillance) so isolating wireless connectivity in a device at all times when not in use is advisable. Pattern of life data can provide useful data to the hacker to support a subsequent targeted attack on an individual device and then subsequently to the home network it connects to.

Wi-Fi is not the only wireless security issue. Bluetooth has been adapted to make remote devices more easily connected. This has been adopted to make it easier for accessories (and in particular handsfree headphones) to be connected but leaves an unsecure gateway into many devices. This is a more prevalent problem for phones but most computers are susceptible to the same risks.

Everybody who uses a digital device is susceptible to this risk however sophisticated hackers would normally target an individual or organisation for gain. This could be sponsored by a sovereign state or criminal gangs and the ultimate goal is likely to be to gain covert access to an organisations network rather than the individually targeted computer.

The state sponsored threat is clearly higher for international business travelers and diplomats. Restricting wireless connectivity directly to a 3G or 4G data network can add a layer of security however this will not defend against state sponsored hacking and in this scenario devices should always be shielded whenever they are not in use at a secure location. If it necessary to connect to a phone network, restricting this to 4G will also give additional protection as it has more security features than the GSM, 3G, CDMA and GPRS.
It should also be noted that a hacker targeting a specific organization is likely to attack a senior officer or official as they will have access to more security layers in their organisation if the network is breached.

It is the challenge for the IT and Security teams to make the life of hacker as difficult as possible and a faraday shield for every digital device used by the mobile workforce will be a simple but effective addition to the arsenal of protective measures.

FARADAY SHIELD DESIGN CRITERIA AND BEST PRACTICE

Having assessed the threat and decided to introduce a wireless shielding solution for your mobile workforce what type of faraday bag do you need?

Clearly the key criteria is an enclosure that will restrict all types of wireless intrusion to a device however there are other factors to be considered including robustness, reliability, longevity, ease of use, cost, aesthetics and physical protection of the device.

To ensure the mobile workforce use the shield effectively the solution will benefit from all the best features of a laptop bag or sleeve but with the additional benefit of isolating the device from the wireless frequencies covering Bluetooth, Wi-Fi, GPS and all mobile phone networks.

An example of why the aesthetics is important can be supported by the recent media coverage of the Brexit Secretary carrying a large aluminum faraday briefcase. This highlighted the fact that there is sensitive data on the device contained within it and would attract the attention of potential hackers. A bag that does not outwardly exhibit any special features is therefore desirable.

Design considerations

Faraday bags are designed to isolate a device from a wide spectrum range of RF signals with the highest possible dBm attenuation* margin. Having made the investment in a shielding enclosure the user will want to ensure it is fit for the purpose.
Products aimed at consumers are typically countering RFID connectivity only and will not offer adequate shielding from all wireless technologies. Also, the product needs to look the part which in most cases is robust construction using a black woven exterior material. This traditional style and material will meet most user expectations though manufacturers should be prepared to tailor a bag or sleeve to meet specific customer requested features and branding.

**Attenuation is an important consideration in the modern world of wireless communication. Attenuation limits the range of radio signals and is affected by the material it must pass through.*

Product design

Having established that the design needs to look like a commercial product the specific design configuration to ensure effective shielding can then be considered.

Closure Method

Traditionally faraday bags have used a rolled-up top to fold over the metalized surfaces to ensure effective shielding however this is unsightly and inconvenient. A bag that closes with a single flap design, (Fig 1) like an envelope, is certainly more convenient as long as the design meets the shielding requirement.

Fig 1 Single flap design closure.

Material Layers

Faraday bags made with a single layer of faraday fabric are unlikely to shield all wireless signals in all situations (specifically 4G and Wi-Fi). It's important to achieve a high level of shielding with multiple layers of fabric on each side. Flat bags will typically have four layers in total.

Faraday Fabric Material

Not only is it important to have dual stitched seams, but the types of materials are also imperative to the effectiveness of any faraday bag. The best metallised fabric is made of highly conductive metals such as silver and copper (Fig 2) These metals are not cheap, so a high-quality faraday fabric is not either.
Some materials use alternative metals such as tin or nickel however these are less conductive. Less conductivity results in less effective signal attenuation (Reduced shielding).
It should also be noted that inserts or liners that use anti-static bags (or metal-coated plastic bags) will not offer high shielding and are not robust enough for this application.

Fig 2 Metalized fabric enables the manufacture of lightweight faraday shielding.

Typical product configurations

Once it has been confirmed that the manufacturing materials will deliver the right levels of attenuation and shielding designs can then be configured to support the most popular wireless products e.g. phones, tablets and laptops.

Laptop bag

These come in a variety of sizes and configurations. Typically, the main shielded enclosure is designed to fit laptops commonly used by the mobile workforce including handles, carry straps and additional pockets for power supplies (Fig 3).

Fig 3 Standard design configured for the Dell Latitude 5280 or Microsoft Surface Pro (Version 2,3 and 4)

Laptop sleeve

Alternatively, the Faraday Shield can be configured as a sleeve that then fits in any commercial bag (Fig 4).

Fig 4 Storage sleeve designed to exact dimensions of the Microsoft Surface Pro (Version 2,3 and 4)

Storage sleeves

Storage sleeves can be designed to protect all phones, tablets and laptops. Additional features such as carry straps and belt or webbing attachment points can be added (Fig 5).

Fig 5 Different sizes sleeves are available depending on the device being shielded

TESTING/CERTIFICATION

What criteria should be used to ensure an effective level of shielding? Assessment by independent authorities has established that attenuation of 50dBm* across all wireless frequencies will give the necessary protection with a margin of safety and anything less may offer some level of protection but doesn't counter the risk of close proximity to a cell site or a modified wireless system with boosted power designed solely to defeat shielding solutions. The power output and receive sensitivity of standard wireless systems is mandated by international regulation however developing radios that work outside of these parameters is well within the capability of the hacker with limited understanding of RF device design.
A professional forensic faraday bag will cover all the current generation of wireless frequencies. Testing to confirm the signal attenuation across this range of frequencies and supporting this with an independent design verification is an essential requirement that should be included in any procurement specification.

Faraday bag testing *continued;*

Typical professional faraday bag test results showing the 50dBm criteria met across a range of wireless frequencies. See Fig. 6.

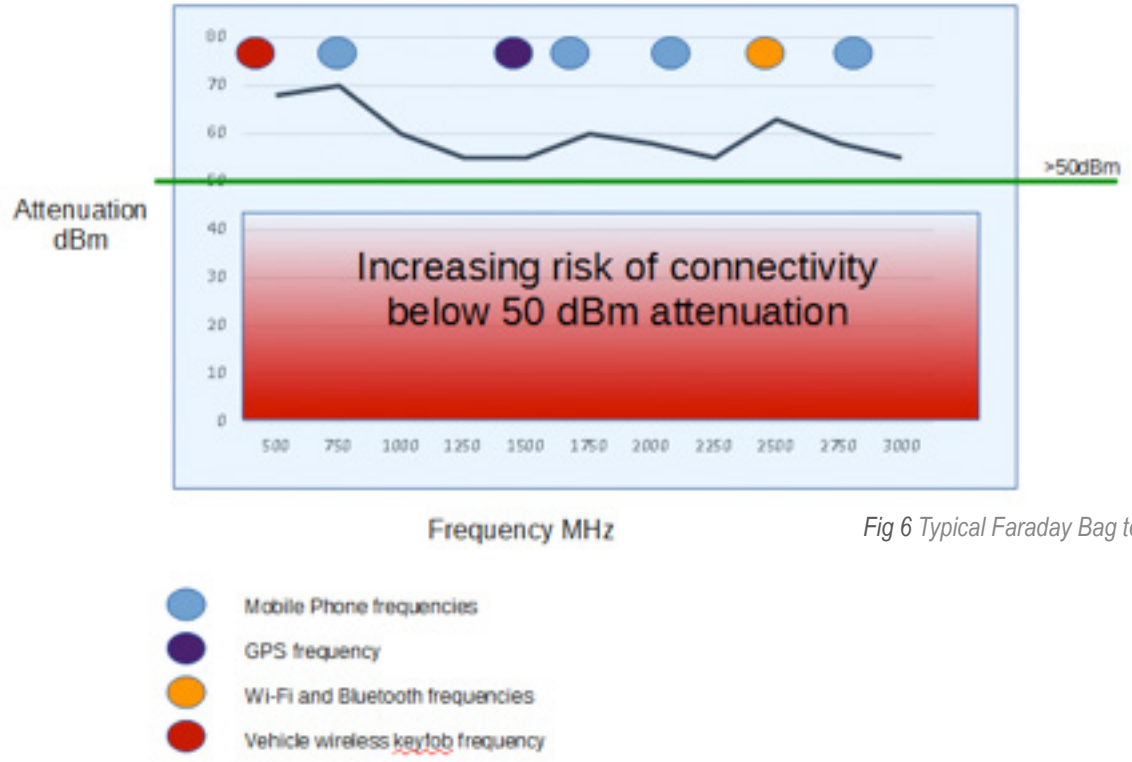

Fig 6 Typical Faraday Bag test result

Other generic standards such as ISO 9001 should be required of the supplier to ensure consistent quality and shielding verification should be carried out on every bag prior to delivery. Cheaper products may use random sample testing. This should not be accepted.

Maintenance and Support

If a high quality metalized lining material is used this will ensure reliable long-term resistance to general wear and tear. If the lining material has an obvious rip or tear in the metalized fabric it should be repaired as soon as possible. Using a double layer of metalized material mitigates the risk that the shielding will be less effective if damaged.

It is also recommended that the faraday shield is periodically checked to confirm shielding performance. Reverifying the performance is a relatively simple procedure. For phones and other 3G or 4G devices simply connect to a network, place the device in the shield leave for 20 to 30 seconds and then try to connect to it. (Call it). The phone should have no service.

The same procedure can be applied to tablets and computers on Wi-Fi or Bluetooth networks. Connect the device to a trusted network, then place the device in the shield for 30 seconds and then remove. A review of the connectivity logs will confirm the device was isolated when placed in the bag.

Special features and branding

There may be a requirement to add special features and Disklabs will be able to advise on the design feasibility. Many organisations issue branded products to their staff and customers. This can be incorporated into all designs.

CONCLUSION

Public wireless networks are increasingly widespread and as a result the use of these to gain unauthorised access to computers and networks in the mobile workforce is becoming more prevalent.

By isolating a computer or tablet from wireless RF signals when not in use will significantly reduce the risk of an illegal attack.

Until recently the incorporation of Faraday shields into enclosures used to carry wireless enabled devices has been mainly adopted by Digital Forensic Specialists, Military and Intelligence users. The development of cost effective shielding solutions that mimic the style and usability of commercial bags and sleeves will overtime become the standard for the mobile workforce.

ADDITIONAL RESOURCES

Disklabs Limited
Galena Close,Tamworth,Staffordshire, B77 4AS

http://www.disklabs.com

Professor Alistair Duffy
BEng (Hons), MEng, MBA, PhD, CEng, FIET, IEEE Fellow, FRSA. De Montfort University

http://faradaybag.com/faraday-testing

For more information;

Mr Andrew Tilbury
Disklabs Limited
Galena Close
Tamworth
Staffordshire
B774AS

Tel: +44 (0) 1827 50000
Emai: at@disklabs.com