

Digital espionage and physical techniques

as the digital age evolves still exists physical threats whether your’e walking your dog or locked in a secured bunker

Andrew McGuire | Security | 02/15/2019 version 1.0 – amcguire2500@gmail.com

# Audience:

This document is meant for those of cyber intelligence and organizations. This is not a complete guide nor a tutorial, it is documented based on personal research both my own and of others. As 2019 turns its curvature towards the sun on earth there is an actual threat to profits, data, intelligence and many more. My intentions within this paper are to expose the ideas and possibilities that not many consider and give an insight on how important it could pose an actual threat to everyone.

## Disclaimer

I am in no way affiliated with the US government as of the date of this paper states. Using the knowledge contained within this paper explains in detail what I’ve personally researched and discovered within all entities and organizations. The purpose of this document is to inform security researchers of my own findings and to help prevent further issues.

The title of this document may change due to the nature of the information disclosed and the original content may be redacted due to the nature of the research depending on the copy, author and the region it was obtained from.

*I dedicate my research to the patience and loving heart of my sweet wife, without you my love I would be lost.*

## the phyiscal layer – A door into the infrastructure

The physical layer has always included the “human” aspect, this is the most vulnerable layer when it comes to the security of the organization or entity. As system software improves so does security however the client facing side of the organization does not get taught the engineering aspects of security in most cases. Breaches occur or data is leaked is never is by the systems holding it or protecting it. It is imperative that every device used within a company has the administrator layer disabled, Not only because you may potentially have an employee stealing data or trading secrets but you also you will have attacks on this layer usually in the form of a malicious document embedded with a payload and the user unexpectedly opens the document and thus compromising the entire organization. Malicious websites are always easy entry points, One can clone a legitimate looking login page and send a the link to the target, the email is formatted in a case such as for example

*Dear* [*username@email.com*](mailto:username@email.com)*,*

*Please login and reset your password to prevent it from expiring within 7 days.*

*http://evilsite.com/auth/login/resetpw*

*IT Department*

Of course evilsite.com will not say “evil site”, there exists a flaw with how outlook processes #&806; and it can mask evilsite.com to appear as company.com. I will not explain how in this document because this is not a tutorial.

Other ways of masking the site for example lets use a random company name “powergrid-security enterprises”. Let’s demonstrate another method using the company’s name within it’s website.

*Dear* [*username@email.com*](mailto:username@email.com)*,*

*Please login and reset your password to prevent it from expiring within 7 days.*

*http://powergrid-secutry/auth/login/resetpw*

*IT Department*

Can you tell the difference? Would you be able to spot the method used in a fast-passed high demand work environment when you have 20 other emails to get through?

Some would however most will not, When a phishing attempt is launched within an organization or entity at the very least its always a 30% or even more that someone fails to notice I left out the “i” within the second example, thus forwarding the unaware victim to supply credentials which then are harvested on the back-end server hosting the fake page and they are redirected to the actual site after to prevent suspicion.

A more advanced technique would to send emails out after researching the company, maybe even making friends with on inside and to take them out for drinks. This is your opportunity that will usually lower a self-defense shield and with alcohol involved if you analyze and use “word judo” which is a technique that allows someone to word their questions in a way that the victim doesn’t even realize they are giving away details that are putting company assets at risk.

For example:

*Attacker hangs out watching how people enter a building, he also notes vehicle plate numbers down to get an idea of the registered owner. He notices they use a keycard to open the door, then he knows he must clone a copy of the key fob or knows he needs to launch an RF scanner to try and tune into the frequencies used and he records them. He knows if he can either decode the frequencies used and reprogram his own card for physical access. If he can amplify that frequency using an RF transceiver such as hackRF and replay attack the access fob reader. He then can find a victim to “just bump into” and even stealing a fob or access card, people lose these everyday anyway so it would alarm the average personal. Then in a hurry by using an android phone with NFC enabled or a portable fob decryption tool he can take the stolen card and do all this within minutes and then pretend to say he saw the victim drop it, and there is his conversation starter. Maybe after that he strikes up a conversation about the job duties the victim has within the organization, or maybe the attacker is a gorgeous woman and the victim happens to be a single man and she asks if he would like to go on a date.*

This is an attack on the lowest level, after the drinks then questions like

*“So how many doors do you even have to use this weird key for? That’s so cool you can use things like that to unlock doors, Technology is so strange to me”*

The attacker now has a door count which he will use in his calculations because the main goal to get access inside would be to find a way to bug the building such as inserting something into an active ethernet outlet that’s PoE and very small, possibly even posing as maintenance once he’s in and take the outlet out and insert the bug on the back side of the outlet so it’s even more stealthy. Adding in “sticky port rules” would block this attack unless the attacker knew the MAC address that was allowed on the port and then spoofing that on the hardware layer of his bug whether it’s a soft spoof and hard spoof.

If the attacker knows sticky port is enabled or even considers it he can then find an open office and quickly add a GSM enabled network tap/bug and intercepting the RX and TX lines of the ethernet cable itself. Then the attacker would be able to remotely gather data and depending on the functionality of the bug he could even make his own the not only allows a tap on a line but also transmit and receive from the line itself by the means of packet injection. He would now can now compromise the entire organization and funnel out data at an alarming rate so that he could process this to locate usernames, email, security attack vectors, how someone words their emails and much more. He could then launch a new attack using only the wording format someone and spoof an email containing a document “reimbursement report.docx” and sending this to someone within accounting.

Specially crafted “homemade” bug not yet been analyzed by anti-virus companies so there would be no detection but through the company’s email filtering system and the company’s virus protection software because the signature of payload has never been analyzed yet to even produce something that would trigger an alert.

Locking down each organization’s users access levels to only their job description is one way to prevent attacks from spreading or access to an organization’s stored monetary data.

This is way it’s very important to implement phishing campaigns continuously so you can educate people who would otherwise fall victim to such attacks.

There are other ways to also prevent even the most advanced attacks as having gated guard posts to check IDs before allowing access into the parking lot and growing tall shrubs to block outside access from using a telescopic device from peeping in without having to deal with the gate. Shrubs will also help hide vehicle tags thus limiting the attacker’s ability of getting information that would be an asset within his main goal.

Having two key fobs, one to get into the building and then you swap that one out for one that is at the front desk. This eliminates the ability to clone the one that will grant full access into the building and will help eliminate the physical placement of the network tap and limit access to sensitive areas like a server room.

Placing EMF material inside the building would help prevent the attack to wirelessly record the frequencies used to open the doors.

If you company MUST use WiFi then enterprise login and encryption must be used, and the broadcasting of access points should be turned off. The MAC addresses of the access points should be cloned so that wireless exploits known for certain brands or models will not be disclosed within the national MAC address registry database. I **strongly advise** never using WiFi and no other wireless technologies such as the very insecure Bluetooth protocol. It wouldn’t be hard to place a small ESP8266 enclosed within a water proof solar panel lithium ion battery powered small device could be flown in with a drown or even as simple as tossing it over a fence could run for hours if not days and perform many wireless attacks such as “WiFi Pineapple” or could get the PMKID’s of the access points if your organization is larger and mesh networks are roaming for better performance then one could get a PMKID in seconds and then the data using GSM could be transmitted to the attacker and then later could use software such as “hashcat” to crack the data. These devices can be made under 5$ but could cost an organization million’s in damages. That’s why depending on what you are wanting to protect I strongly disagree with a wireless work environment and would invest in hardwiring the network to each end point. If WiFi is used it MUST be separated and placed within its own VLAN however you still risk packet injections, and much other wireless types of attacks. Say an access point was compromised, a top-level executive gets ready to leave the office and gets all the way down the hall realizing he forgot to send out that late Friday email. He thinks “I’ll just send it here because there is a WiFi connection I can use really quick”

Weekly if not daily vulnerability scanning should be used to scan all connected devices and if possible, have new devices that connect scanned to ensure a compromised system does connect and disconnect before the automated scan can run.

***It only takes one time, someone once told me “The knock of opportunity only knocks once” If you want in chances are you go right for the individuals inside.***

## the network layer – A road for data adventures

As previously discussed within the physical layer and how a network tap could pose a threat, or a wireless transmission could be injected. Having a strong network defense is vital, if you do not have a strong network within the organization then you might as well leave the doors unlocked and the safe open.

Having sticky ports to block unwanted MAC addresses from connecting would block a non-authorized device from connecting to the network. If this is bypassed with advanced attack features the attacker now can do many of the following:

* Data sniffing
* Password harvesting
* Unpatched system compromise
* Spread malware to more devices
* Packet manipulation
* Identify spoofing
* Compromise security keys
* Denial of service
* Database leaks
* And much more

Such attacks are as easily performed you could do all of this with a rooted android phone and just a few app if not a single app.

Based on what I’ve witnessed personally is the attacker get inside the network its time to call the insurance company. If you are in need to maintain PCI compliance and/or GDPR you’ve already lost your compliance statuses, and this will not only hurt you but also your clients which will open you up to a massive lawsuit or lawsuits depending on how bad it is. Smaller companies are working hard enough to continue to operate so the funds on security are usually dismissed because we need to fly “Joe” to LA for a week to have dinner with a few clients. That single trip alone would be the price of an automated scanner “Nessus” that would be much more worth the trip “Joe” has to take or funds should be shifted around and planned for before “Joe” schedules his trip. If “Joe’s” trip was a success however you’ve lost your compliance statuses, then “Joe’s” trip was worthless and then turns into a monetary issue.

Id highly advisable that you appoint a CISO over your organization whether large or small IF you need to maintain security over the data you collect. A CISO is a chief information security officer and his duties would be to maintain the security of the entire organization whether network layered, application layered, system layered, physical layered and much more areas including undiscovered ones. It would be his role to manually test and try to find these undiscovered attack vectors and even manually test the known attack vectors so you would need someone who is passionate about security and doesn’t just read a book on it but stands up controlled environments to prevent leakage and does their own testing.

What I enjoy doing even on my free time is building out an application/webserver, mail server, basically every aspect of a normal organization infrastructure and then I go in and harden it. My next job is to see if even I could get into it, I’ll use password generation techniques, so I won’t know any passwords, random IP addresses and MAC addresses. My goal is to build it without knowing anything about it and starting my research from the lowest level whether it is giving a SSH PEM file on my wife’s laptop without her knowledge and phishing her into allowing me to add a dropper to her laptop without her knowledge and gather the files and information I need in order to start planning my next attack. Hands-on testing is extremely important which goes back to my phishing campaigns. (she knows about security also because of how dedicated I am to it she has had to deal with internet outages while wanting to read online books – not on purpose)

There are many ways to help defend against network-based attacks, one if hardware firewalls, packet filtering, intrusion detection systems, file monitoring/triggering alerting systems and others. I couldn’t explain all the technologies available without writing a 10,000 page manual on each type.

I’ve also noticed it does no good to have the same firewall behind the same firewall, While working on a project for the DoD the network guy put 15 Cisco ASAs in front of the WAN, routing and NAT’ing each static IP through that was a nightmare, however he did have a good idea but where it flawed is when that Cisco ASA has a remote RCE released into the wild then all 15 of those firewalls turn into a wide-open router only. So it’s recommended to use different types of devices between them such as packet filtering devices between the firewalls and maybe even a simple tap between them to alert the network team something is flowing through the lines that doesn’t seem normal.

It’s also highly recommended to have all internal incoming communication on its own dedicated VPN for encrypting and to have all internal outgoing on a dedicated VPN. If you transmit and receive using the WAN then place the same outgoing and incoming configuration for that as well and put all on their own VLAN to prevent any cross contamination.

## the Application layer – the face your company shows to the world

With a strong infrastructure and you do not offer an interactive application your security will now be secure. For example, a local gas station isn’t going to rely on application they are selling or hosting to make money. If you do develop applications then you must focus on code security, most of the worlds data leaks and stolen identities were due to bad programming practice or non-sanitizing input data properly. Even the worlds best coder could run out of coffee and have an EOD deadline but need to write 500,000 more lines of code. This goes back to the human aspect, we all make mistakes however having an automated correctly configured code scanner to scan the code before it was ever released into a production environment would provide an extra layer of security and be a safety net for the programmer in case, he forgot to add sanitation to an input field in his PHP code. Even with a 1 million dollar firewall, if the PCB board was accessible and the components were labeled one could find a way to short circuit the IC and drop the attacker into a shell, there’s other methods such as soldering a console cable to the chip itself or using jumpers to bypass but I will not explain that because that’s a responsibility of the electrical engineer of the manufacturing company of the actual device. I provided that as an example, but what this focus is on the grounds that even adding security into your applications that prevented shell access completely is the goal! For example:

***If you build applications that are flashed onto chips, or websites it very important to disable the root access or administrator level access and when you need to apply changes to even the system layer itself then you push out updates. So you build your application and the system it runs on to accept firmware/software updates in order to change system level settings or to update firmware for drivers the system uses but disabling root level access will be another line of defense.***

It is also highly recommended to have a scanning software that doesn’t scan the actual code but scans the running application, SQLi attacks, XSS, crafted packets and etc.. It is also a CISO’s duty to manually test the applications inputs, for example a specially craft DHCP packet sent to a router, firewall, switch could cause a denial of service or even worse shell level access.

## the system layer – the foundation running your product

System security is a very high priority whether you build and sell devices and applications, if the system running it crumbles with an attack it will take everything else down with it. Its extremely important to maintain security patches and updates to the operating systems within your organization or your product. This also gives added bonuses because an engineer will know how to optimize the system’s kernel and thus improving your network stack, application responsiveness and much more. Automated scanning system components, system configurations, file permissions, configuration file locations, system users all should be considered. If you have a website running and you applied all the patches, harden the system however have NGINX or Apache2 running as a user that has shell access and the PHP files serving the content if an attack finds an injection and they are dropped into a shell all that hardening and patching was done in vain. Its vital to maintain secured systems whether it’s the laptops the organizations employees use to the server hosting your application. All input fields should be manually tested regularly, sometimes automated scanners will not pick up human findings. Its also recommended to prevent USB drives from being inserted into them, locking the BIOS, limiting non-administrator users access to what is only vital to their role within the organization.

## the closure – every section can relate together and work together

Every aspect of the infrastructure plays a role in each of its subsections, you could send a malicious file and it’s opened by an employee and that single file could open every layer of the organization to all kinds of threats. Security engineering shouldn’t be viewed just as electrical engineering shouldn’t be only a power outlet. They both have subcategories or areas to research, RF frequencies are apart of electrical engineering, using both together an attacker would pose a very strong threat. Like cloning garage door openers using an RTLSDR and GQRX to record the frequency and then decoding it into digitals and use to reprogram another remote and then the attack can open your garage by just using electrical engineering radio waves and his knowledge of decrypting data. I have taken personal interest in electrical engineering because understanding the hardware layer can help me build a secure future.

Thank you for reading, I am currently looking for security positions or contracts, I have many years both self-research and trained professional research that I use within my thought process. I worked within government projects and private companies doing both system administration toe DevOps to DevSecOps for over 8 years.

*Sources:*

[*https://carnegieendowment.org/files/GUP\_Perkovich\_Levite\_UnderstandingCyberConflict\_Ch1.pdf*](https://carnegieendowment.org/files/GUP_Perkovich_Levite_UnderstandingCyberConflict_Ch1.pdf)

[*https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-62-no-3/pdfs/io-bookshelf.pdf*](https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-62-no-3/pdfs/io-bookshelf.pdf)

[*https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-62-no-3/pdfs/studies-sep-2018-unclassified-extracts.pdf*](https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-62-no-3/pdfs/studies-sep-2018-unclassified-extracts.pdf)

[*https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf*](https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf)

[*https://warwick.ac.uk/fac/soc/pais/people/aldrich/vigilant/espionage\_and\_intelligence\_viewpoints.pdf*](https://warwick.ac.uk/fac/soc/pais/people/aldrich/vigilant/espionage_and_intelligence_viewpoints.pdf)

[*https://www.easyredir.com/blog/why-you-should-not-use-url-masking-forwarding-cloaking/*](https://www.easyredir.com/blog/why-you-should-not-use-url-masking-forwarding-cloaking/)

*<https://www.techrepublic.com/article/microsoft-office-is-more-dangerous-than-you-think-doc-deliver-45-of-all-malware/>*

[*https://www.thebalancecareers.com/how-to-check-emails-for-fake-hyperlinks-3515356*](https://www.thebalancecareers.com/how-to-check-emails-for-fake-hyperlinks-3515356)