BIZCOMMUNITY

# Deep packet sniffing, penetration testing and vulnerabilities: A guide to modern IT security

By Colin Thornton

16 Nov 2017

Yes, I know what you're thinking...this sounds like some kind of twisted geek version of *Fifty Shades of Grey*. And while I hope our message can instil the same kind of reader and media frenzy as that soft porn novel and film, it is admittedly a far more sombre (and arguably far more important) topic for discussion: IT security and mobility.

Though it hasn't quite broken the traditional security paradigm, mobility's done a decent enough job of warping the entire landscape. For you, the end user, it's worth paying attention to unfolding developments – and finding out how you can become more secure.

## Boundaries, what boundaries?

Today's security teams must defend against far more than the odd intrusion attack or malicious app. Arguably, as with soft porn (yes, *Fifty Shades of Grey*!) and sex on social media, traditional boundaries and security perimeters have all but dissolved, and threat surfaces have broadened significantly.

This means that in today's world, there are multiple levels at which your organisation can be compromised – and you need to layer defence at each one…

## Network level – borders have their limitations

Network-level security comprises mostly everything on the 'traditional' security front – firewalls, authentication, and network encryption, to name a few. These tools are still essential to securing your enterprise; new threats such as spear phishing attacks and unsecure file sharing don't negate old-fashioned ones like traffic flooding or buffer overflows.

At the same time, however, network controls on their own aren't sufficient. A firewall may keep an attacker out, but it can't protect files outside its perimeter. Encryption may protect network communications from intrusion, but it doesn't stop a careless employee from forwarding an email to someone who shouldn't be reading it.

## Device level – attackable and hackable!

In addition to network-level security, device-level security is one layer that most security teams already cover. Passwords, full-drive encryption, and device containers are all incorporated into most user devices to one degree or another. Microsoft's BitLocker, for example, allows the user to harden an entire drive against intrusion, while Samsung KNOX allows the creation of a separate work and personal profile, walling corporate data off from private.

As with network-level controls, device security is necessary, but it also shouldn't be your only line of defence. Hard disk encryption can be broken; passwords and PINs can be cracked. And device-level controls aren't always reliable, either – they vary by device and manufacturer.

## Application level – containers are important

Malware aside, unsecure applications represent a significant risk for businesses, particularly those with burgeoning mobile initiatives. Data leakage remains a consistent threat, with 46.2% of apps on iOS and 86.7% of apps on Android exhibiting privacy-invasive behaviours, and user privacy is an ever-growing concern.

By locking down your business-critical apps with a device-independent containerisation tool like that used with SonicWALL, you can keep your organisation's data safe from bad apps and physical theft.

## File level – your last line of defence

Finally, we've got security controls at the file-level. Even if an attacker somehow manages to crack a device or make it into your network; and even if a negligent employee shares documents with someone they shouldn't, file security represents a second layer of defence. It ensures that even if your critical files leave the firewall and wind up in the hands of a third party, you never lose control of them.

Encryption can be broken – and if encryption is all you rely on - if you have no secondary protections - that means your data is at risk. With a multi-tiered approach to security, you can protect yourself at every layer. You can encrypt the hard drive and network communications, and place apps within the secure container.

(While this is definitely not *Fifty Shades of Grey* or a smutty Barbara Cartland novel, we certainly think it's an important message to consider for both you and your business…)


### ABOUT COLIN THORNTON

Colin founded Dial a Nerd in 1998 as a consumer IT support company and in 2002 the business- focused division was founded. Supporting SME's is now its primary focus. In 2015 his company, merged with Turrito Networks who provided niche internet services outside of the local network. These two companies have created an end-to-end IT and Communication solution for SME's. Colin has subsequently become the managing director of Turrito. Contact him at info@dialanerd.co.za

- Understanding SA's 5G reality - 4 Apr 2019
- Why your business needs a cloud architect - 21 Feb 2019
- Privacy vs Profit: Will 2019 be the year of consumer paranoia? - 26 Nov 2018
- Why SMEs should be looking at cyber insurance - 28 Sep 2018
- Why your future digital ID should harness blockchain technology - 23 Aug 2018

View my profile and articles...