
# BSidesMCR Conference

**29/08/2019**

**Abstract**

BSides is a community driven event built for and by information security community members. BSidesMCR held the 6th occurrence of its annual conference on the 29th August 2019 and this report will outline my experience and learnings from the day, with some in-work applications. NB: Opinions are my own and the statements made about vendors/software/hardware are correct as far as I'm aware.

**Miles Eastwood**

# HTTP Desync Attacks: Smashing into the Cell Next Door

## By James Kettle - PortSwigger (@albinowax)

This presentation explored the techniques for remote, unauthenticated attackers to smash through the traditional view of HTTP requests as isolated, standalone entities and splice their requests into others.

Since HTTP/1.1 there's been widespread support for sending multiple HTTP requests over a single TCP or SSL/TLS socket. The requests are placed back to back and the server parses headers to work out where each one ends and the next starts. Figure 1 shows a multi-tiered architecture and takes HTTP requests from multiple different users and routes them over a single connection:

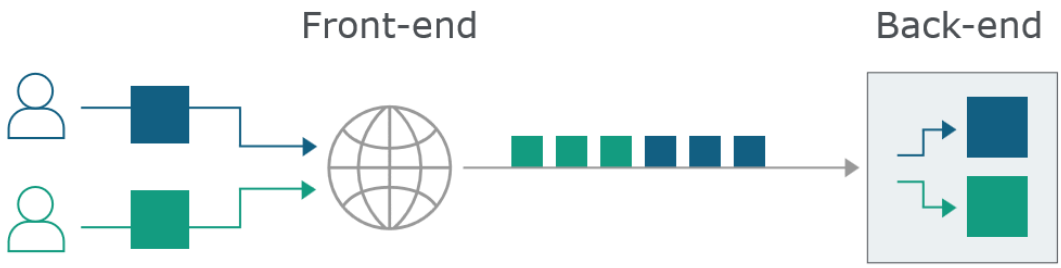


**Figure 1 - Multi-tiered Architecture**

From Figure 1, it can be seen that agreement between the back-end and front-end is crucial as this indicates where each message ends. Otherwise, an attacker can send an ambiguous message which gets incorrectly interpreted:

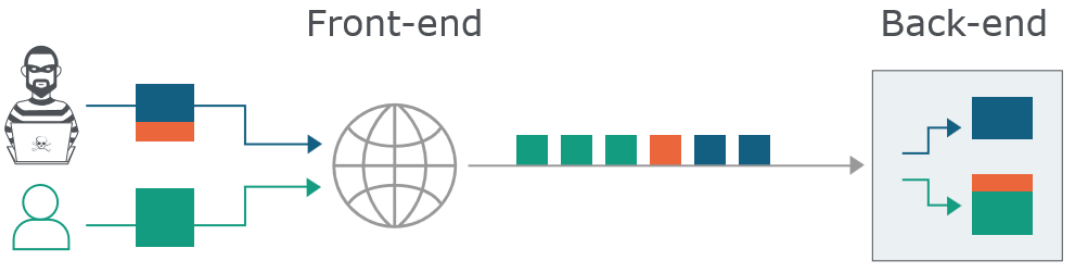


**Figure 2 - Ambiguous HTTP Request**

This gives the attacker the ability to prepend arbitrary content at the start of the next legitimate user's request. The introduction of the orange data leaves the back-end socket poisoned; when a legitimate request arrives an unexpected response is caused.

Whilst it only appears to be a disruptive attack from Figures 1 & 2, HTTP desync attacks have been successfully used to smuggle malicious HTTP requests into the legitimate – earning the presenter over $70,000 in bug bounties. Most notably this attack was proven able to retrieve passwords from PayPal, who paid out twice as they were susceptible to the attack with a slight syntax change after remediating from the first bug report.

Determining the vulnerability in a web service can be done either by sending an ambiguous request immediately followed by a normal 'victim' request and observing the response or by using PortSwigger's BurpSuite for web vulnerability testing (N.B. the presenter works for PortSwigger).

Further reading on the use of HTTP desync attacks can be found on a blog on the PortSwigger website.

## Hacking RF: Breaking what We Can't See

### By Grant Colgan (@Brains933)

The presentation looked at how replay, repeater and man in the middle attacks worked with Radio Frequency (RF) using kit that could be made extraordinarily cheaply using parts from Amazon (10 single use kits would cost roughly £7).

Wireless entry car keys are particularly vulnerable to repeater attacks as the signal from the key can be relayed by a device and extended to allow the car to be stolen without needing the keys. An example of this is caught on CCTV.

It was thought that using a rolling code would prevent thieves from stealing cars so easily. For example, on the first key press the code would be 001 and increment from there. However, using a roll jam defeats the rolling code.

A roll jam works by introducing a device in between the keys to the car and the receiver on the car. When the keys transmit the unlock code (001), this is captured by the device and a jamming signal is sent to the car and the key – preventing the car from being unlocked. Individuals will then try multiple attempts to unlock the vehicle, each code is captured and the signal jammed. The attacker can then use the device to unlock the car and drive away – as well as have a bank of unlock codes to use if they are subsequently locked out.

The presentation then also explored how the attackers could also be used for Internet of Things (IoT) devices, industrial equipment (e.g. cranes) and medical devices.

With industrial equipment, an attacker could sit and capture the various input signals and monitor for their impact (e.g. 002=left, 003=right etc.). These signals could then be replayed to control the assets using a specific bandwidth. It is often assumed that encryption would be the answer to protecting the asset, however with the signal and understanding its impact the attacker need not decrypt it – the asset will decrypt it for them and carry out the instruction from the signal.

There was a story told about a company who told the speaker that the signals were encrypted so there were no concerns about security. He captured all the signals for the remote control crane, went back to his hotel room and then proceeded to remotely drive it round the company's carpark.

## Getting Splunky with Lateral Movement – Attack, Detect and Evade

### By Ross Bingham and Tom MacDonald - NETTITUDE (@BaffledJimmy & @PwnDexter)

In this presentation it was explored how attacks could be made, how Splunk could then detect and report upon the attacks and how then the attacks could be amended to evade detection from Splunk.

It was interesting to see that the dream of collating every log possible and having Splunk process it, would only serve to be detrimental. Too much information could, without proper resources, knock the Splunk service over as it cannot process the sheer amount of information it is passed. With too much information Splunk becomes a difficult tool to use as the number of logs drowns out the events of concern.

The main takeaway with regards to Splunk was the importance of setting the right configuration to meet the requirements of which drove its adoption and implementation.

Evading Splunk started off simple with techniques such as changing the name of the service used by the attack to something inconspicuous such as 'Citrix Updater', to the more technically enhanced such as spawning processes from the initial service and distributing the attack.

In summary of their presentation, the concluding statements included "don't be an armadillo" and that the introduction of honey systems was the future.

Armadillo was used as a term to describe networks/systems that are hard on the outside but soft on the inside.

## Threat Modelling and Black Swans – Predicting the unpredictable by thinking like an attacker

### By Nick Dunn (@N1ckDunn)

Some IT security risk assessments tend to only identify technical threats and whilst this is arguably the bulk of threats to a systems/network, there a 'blind spots' left behind.

The flow of the risk assessment usually follows:

- Identification of the assets.
- Identification of risks posed.
- Mitigations of the risks.
- Identification of the residual risks.

And to identify threats the modelling technique STRIDE is used – Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Escalation of Privilege.

The 'Black Swan' process seemed to be a re-application of the STRIDE modelling technique but used in 'non-technical' circumstances and primarily focussed on the physical. Nothing particularly ground breaking as covering elements that aren't just IT should be part of a well thought out risk assessment anyway. Within the organisation and the assessments that are made, they should encompass all possible risks as to present the complete case to the risk owner.

## Nice Vulnerability, I don't care

### By James Carter (@tenbellycarter)

The presentation opened with questions posed to the audience about their experience of dealing with their respective businesses with regards to risk and vulnerabilities. Discussions focussed on organisational inertia and feelings of being stuck in an information security chamber.

Instead of a talk about the management of vulnerabilities as the title suggests, this talk was aimed at exploring how information security professionals have a very specific language. This language can make it difficult for the business to quantify the impact to operations and determine how much attention risks/vulnerabilities should get.

Risk was generated using the triangle model in Figure 3:

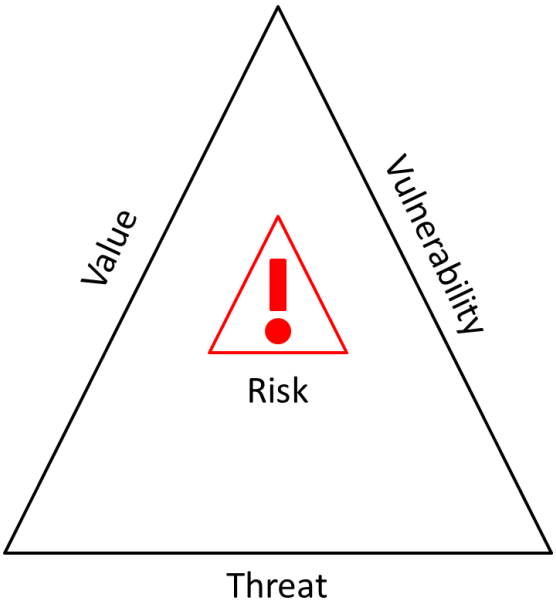


**Figure 3 - Risk Triangle**

The explanation behind each element of the triangle is as follows:

Information has value. Without information, 'IT' becomes expensive tin and services. What it is exactly that makes information valuable can be categorised as intellectual property, regulatory & legal requirements and reputational, amongst others. It is often measured in terms of Confidentiality, Integrity and Availability (C, I & A) which can be useful internally to calculate the value that is discussed with the business. The value of information drives the 'why' behind the risk.

Threat drives 'what'. What could happen is only facilitated by the existence of a threat that could exploit the vulnerability and causes a detrimental impact to the value, thus realising the risk.

Vulnerability can be any weakness that can be exploited as part of the risk and is the 'how' behind realisation of the risk.

The adoption of common business practice for the analysis of risk qualification and quantification was a key point of the presentation. Information Security was likened to Health & Safety for data and the use of an H&S risk calculator for the explanation of Security risk was advocated.

Using Information Security calculations such as CVSS (Common Vulnerability Scoring System) was something to be done internally, rather than communicated to the business.

RISK = IMPACT * LIKELIHOOD

Something that an organisation should have is a risk appetite. This needs to be defined with the business and will inform how much risk/what risks the business is willing to take, what risks require discussion and the risks that are deemed unacceptable. Any decision should be documented and include whether the risk is to be treated, tolerated, transferred or terminated.

There should be a common language to talk to a business with to show them exactly when and why it is important, utilising risk assessments to choose and prioritise actions.

## Protecting Kids Online: Are We Doing Enough

### By Katie Colgan

An interesting talk that did, as the title suggests, cover the topics of protecting kids online but applications and crossovers to business could be drawn from it.

The early years to pre-teen covered monitoring devices (both audio and visual IoT) devices and focussed on how, with malicious intent, an attacker could use access to the device to monitor routines to either carry out robberies or even abduct children. However, audio and visual IoT devices aren't limited in their application to child monitors – a common implementation in businesses is IP CCTV cameras and PID sensors. These, if compromised, can cause damages through being used to monitor events and employees, developing routines that could be exploited to cause damages to the company and/or individuals. Additionally, if availability becomes compromised then that could have legal and reputational repercussions. This all reinforces the view that securing IoT devices in the workplace is critical, as well as in our personal lives which we might not already be doing/be worried about.

Teens to young adults was the next age bracket discussed with concerns over social media, in particular the collation of people's personal information, location data as well as the spread of fake news and harmful content. Social media in reality has an impact across all ages as its use increases at a large rate across all generations; however it is generally believed that those of a certain age are wise enough to the dangers.

If that is to be believed, the graduate/apprentice communities are targeted due to the influence that can be had over them. Social media and the practice of social engineering could be deployed to create inadvertent and potentially even deliberate insider threats. Increasing use of social media by nation states to gather information and targets only proves this – a personal example is an increased number of friend requests on Facebook from accounts of Asian origins at the same time as the Lazarus North Korean APT began ramping up operations.

Social media platforms have access to messages, calls, location data, habits and many more categories of Personally Identifiable Information (PII). This only highlights that for everyone, the control of their information is essential to protect their identity and by proxy, the business itself.

# I like big bots

## By James Maude (@endpointsec)

In the context of this presentation, a bot is something that simulates the behaviours of a real user. To give numbers as to the impact of bots currently, 53% of web traffic is caused by bots, of that 61% is unwanted or malicious and 90% of failed login attempts are credential stuffing (brute force) attacks (figures are derived from the clients of the presenter). A basic bot can be created using a script and a browser.

Whilst bots can be a force for good, they are deployed in malicious and unwanted ways. As basic bots are easy to create, they can be made in bulk and deployed using scripts that can be built up in complexity. Some examples of unwanted/malicious bots are:

- Ticket/trainer snipers:
    - The resell value of tickets to events and conferences can be extraordinary, with the right scripts bots can be used to collect and resell tickets for any amount of profit almost instantly after the release.
    - This also applies to trainers as limited edition, designer trainers are an increasingly sought after item. Bots can be used to buy limited release trainers and resell them, in much the same way as tickets. Also, on websites like StockX (a website which emulates a stock market for designer items) bots can be used to buy items as soon as they drop to specific prices before a real user has chance to.
- Credential checkers:
    - As previously mentioned, 90% of the failed login attempts made to the presenter's clients are credential stuffing attacks. Bots can be setup to try login credentials on web addresses and validate information found on pastebin sites, it is always worth checking whether your address has been pwned: https://haveibeenpwned.com/.
    - Additionally, bots can also be used to check payment information. An example used was a dramatic increase in the purchase of cheese from a wholesaler whereby bots had been ordering to confirm the viability of credit card information found in a pastebin site when a company had been hacked.
- Mirai botnet:
    - Not an example explored in the presentation but is one of the most high profile malicious uses of bots.
    - Mirai is a malware that targets IoT devices running Linux and gains access to them by credential stuffing using common word lists. The infected IoT devices are then controlled by one source and used as a network of bots – a botnet. This botnet can then be used to target networks, using HTTP flood and network-level attacks to deliver a Distributed or sole Denial of Service (D/DoS).

Whilst the simple answer would be to increase the effort required to purchase an item to reduce the effectiveness of bots, at the same time this would increase the difficulties for normal customers and perhaps put them off their purchase. It was also claimed that CAPTCHA, which is designed to tell computers and humans apart, can no longer do just that.

# Fun with Frida!

### By James Williams (@two06)

Frida is a dynamic instrumentation toolkit that can inject into any process and hook into functions as well – all without requiring the source code for them. The toolkit can be used for API hooking to view/modify functions, can be executed before or after the function call and can completely control the program flow. The software is free, open source and currently used predominantly for mobile testing.

In an eye opening demo, Frida was shown to be able to hook into KeePass (an already broken password manager) and capture the plaintext usernames/passwords as they were copied from the password manager entry. All done with no software setup, just a simple command to instruct Frida which function to hook into.

There are a number of Frida components:

- Frida:
    - Python wrapper for the Frida.dll
    - Allows for customer tooling though Python development.
    - All dependencies need to be installed on the host that is being interacted with.
- FridaSharp:
    - C# wrapper around the Frida.dll
    - No dependencies.
    - Completely customisable.
- Frida-gum:
    - C-APIs
    - Still have to be local (although can be achieved through RDP).
- FridaGadget:
    - Shared library injected into process.
    - Communicates with Frida over TCP.
    - TCP listening on localhost (127.0.0.1).
    - Can be configured.
    - Ability to run scripts on start-up.
- FridaInject
    - Injection dlls.
    - Can be utilised with software such as CobaltStrike.

## Market Stalls:

### PwC

The drive from PwC appeared to be a push on recruitment as there was information on both graduate schemes and roles for experienced professionals. PwC also was advertising that they were running an information security consultancy arm of their organisation which is divided into Cyber Security Advisory, Cyber Threat Operation, Identity and Access Management (IdAM) and Network Information Security.

Besides the sales and recruitment elements, there was an interesting report 'Operation Cloud Hopper' which was published in April this year by PwC in collaboration with BAE Systems. The report centres on APT (Advanced Persistent Threat) 10 (Menupass Team) which has targeted managed IT Service Providers (MSPs) with aims of retrieving intellectual property from both providers and clients. The threat actor is assessed as highly likely of being a China-based threat actor. With the specific targeting of intellectual property on a global scale and general espionage activity it is a clear threat to our organisation, especially with growing interest in the Maritime and Defence sectors by other alleged China-based APTs such as APT1 (Unit 61398 (PLA), Comment Crew), APT3 (UPS Team), APT12 (Calc Team), APT18 (Webky) and APT40. The report is high-level and relatively digestible with a separate technical report. Electronic copies of the repot with technical annexes are available from the PwC website – even with md5 hashes for each element for the paranoid amongst us. For more on the aforementioned APTs, FireEye has a good amount of material for each of them and other nation state attributed APTs on their website.

### PortSwigger

The creators of BurpSuite were interested in taking a survey regarding the use cases of their software, which was answered with personal use in virtual machine testing for capture the flags as currently the tool is not deployed on the network.

### NCCGroup

NCCGroup were offering the prize of a new iPad to the individual who scored the most points on their capture the flag, political ballot themed virtual machine. Whilst not attempting the virtual machine, speaking to those running the stall revealed that they were there on recruitment drives for their training programmes.

### MWR

The individuals manning the stalls didn't speak about the services they provide but after some research I found that they are a cyber security consultancy firm that markets and individual selling points as knowledge of the latest techniques and tooling as well as their focus research and technical excellence.

What drew most to the stall was the chance to win a PS4 console and games, as well as the ability to win a t-shirt after successfully picking a lock.

## Elastic

Elastic were marketing their products and solutions which comprised of:

- The Elastic Stack:
    - Kibana – Visualisation of data from Elasticsearch and navigation for the stack.
    - Elasticsearch – A distributed search and analytics engine.
    - Beats – Lightweight data shippers.
    - Logstash – A server-side data processing pipeline.
- App Search, Site Search, Enterprise Search, Logging, Metrics, APM, Business Analytics and Security Analytics.
- Elastic Cloud (SaaS)/Elastic Cloud Enterprise (Self-managed/Standalone):
    - Elasticsearch service.
    - Site Search service.
    - App Search service.

## Pentest

This company was responsible for sponsoring the after party and running a "fastest Mario Kart SNES lap time" for which the winner got a Raspberry Pi arcade kit. The individuals on the stall appeared more interested in the Mario Kart competition and dishing out after party tickets that talking about their own organisation.

## Hackerone

Hackerone is a company that provides a pentest and bug bounty platform, "powered by hackers".