Cybersecurity Education: Key Exercise

James Davenport
J.H.Davenport@bath.ac.uk

University of Bath
Institute of Coding: https://instituteofcoding.org/

7 January 2021

CyberSecurity: two views

1. **"Airline passenger" view**: safety is basically down to the pilots, and the mechanics who maintain the plane, and the companies that build safe aeroplanes. I'd just better make sure I don't book on a dodgy airline.
2. **"Car driver" view**: obviously I'd hope I bought a safe car, but it's up to me to drive it safely, get periodic checks, and deal with warning lights etc.

Our students tend to have view 1: the challenge is moving them to view 2, or beyond, as

- There's no equivalent of vehicle "type approval" for software packages, just "Which Car"-like websites (but cybersecurity advice on StackOverflow is very poor [FBX+17])
- There's no "MoT-like" requirement for periodic checks (except [Pay18, ¶11.2,¶11.3])
- The "rules of the road" change unpredictably

Security Skills we could teach [Pra20]

1. **Risk identification and management**.

JHD Aim to teach ‘risk identification’.

2. **Technical fundamentals**.

JHD Clearly.

3. **Data management and analysis**.

JHD Appreciation for the need for this — this exercise generates 5–100 MiB of data.

4. **DevSecOps**.
5. **Cloud**.
6. **Automation**.
7. **Threat hunting**. [JHD very dubious]
8. **Interpersonal skills**.

JHD Report-writing for a non-technical audience.

9. **Business acumen**.
10. **Agility**.

Bath teaches MSc Cybersecurity

In three formats, but all as "generalist" rather than a specialist Cybersecurity MSc.
All are 6 ECTS (12 CATS) and have a PCI (Payment Card Industry) exercise.

"Face to Face" Full-time MSc (various flavours). PCI 50%, Group Presentation 30%, Exam 20%

Level 7 "Digital Solutions" Degree Apprentice. Cybersecurity roadmap 20%, PCI 30%, Case study 50%.

Online Part-time block mode MSc. Cybersecurity roadmap 20%, PCI 30%, Case study 50%.

* The 30% ones analyse one site rather than 3 for the 50% version.

Full-time PCI Exercise: I (5 March)

"I require each of you to make (or "pretend to make", getting as far as submitting syntactically correct payment card data) three online purchases from different vendors, at least two of which must be commercial vendors (i.e. not government/university websites) For there online purchases, you should collect:

- The web page (i.e. the actual HTML) you were entering the purchase data (Primary Account Number, CVV etc.) into — note that you may wish to save the web page before entering the data!;
- A screen shot of the page (again, probably before data entry);
- The browser's log (typically a HAR file) of the *entire* process, from your starting to interact with the website to purchase accepted/declined;
- The network trace (Wireshark or equivalent), of the purchase process." (where possible)

Full-time PCI Exercise: IIa (16 April)

You should write a report with the following sections

1–3. **Analysis (10 marks each)** in detail of **three** of your online transactions to three different merchants. This should include the following.

   1. With which websites does your browser communicate during the transaction? Are there any that worry you, or whose function you do not understand?
   2. Looking at the logs, to which sites does your payment card number get sent, and how is it protected in transit? You *should* quote the relevant part of the logs, but *should* replace the card number and any other identifying/sensitive data, e.g. by `NNNN NNNN NNNN NNNN`, before quoting.
   3. Looking at the HTML you have saved, do you feel confident you know what it is doing with your data?
   4. How dependent is the HTML/JavaSscript... you have on the correct functioning of the DNS? In particular, could bad DNS results result in a security problem?
   5. What makes you think that the sum of money displayed to you is the sum that will be transmitted to your bank?

Full-time PCI Exercise: IIb (16 April)

4. **Comparison (10 marks)** Your employer is looking to develop a web shop, and has bids from three suppliers. Assume that the three sites you have used are being put forward as examples of their work by the three vendors. **From a security point of view**, write a evaluation of the security features as you see them from these transactions. Are there any suppliers you would defintely not recommend?
5. **Conclusions (10 marks).**
    1. What have you learned about the security of your card data?
    2. In particular, what did you learn from the logs/HTML that you could not have reasonably deduced as a shopper with no access to these?
    3. How obvious is the security of the websites to the shopper?
    4. How might the system be more transparent to the shopper?

Student Feedback

- Three students (out of 32) in the 2019/20 cohort did MSc Dissertations on this subject.
- “I’ve learned a great deal about the process”
- “I had no idea all those sites were seeing my data”
- and many more on the same lines.

General Issues (Naïvety)

- Poor understanding of the DNS, and the fact that `https` certificates should mean that an `https`-only transaction can't be mis-directed.

+ failure to pick up cases where there was some inter-mingled `http`.

- Confusion over Chrome's Security Tools — many students report that it means the site is not malicious.
- An assumption that if they can't see the card number in clear, it's not being leaked

My specific Feedback to part-time MSc

1. 3 of the 14 of you reported connecting to the online-metrix.net site.

   ☡ But only one of you was worried by it. Just because a site has an innocuous name doesn't mean it's innocuous: recall the BA hack and baways.com.

2. One of these was connecting to samis.bath.ac.uk, and I've checked that this site doesn't connect to online-metrix.net (and indeed some-one else connecting to samis.bath.ac.uk didn't have it).
3. This is probably malware. See [Dzh18] or http://uninstallallspyware.blogspot.com/2018/11/remove-online-metrixnet-in-simple.html.

I haven't yet had a response to this.

I. Dzhubanov.
How to remove Online-metrix.net.
https://www.besttechtips.org/how-to-remove-online-metrix-net/, 2018.

F. Fischer, K. Böttinger, H. Xiao, C. Stransky, Y. Acar, M. Backes, and S. Fahl.
Stack Overflow Considered Harmful? The Impact of Copy&Paste on Android Application Security.
38th IEEE Symposium on Security and Privacy (SP), pages 121–136, 2017.

Payment Card Industry Security Standards Council (PCI SSC).
Requirements and Security Assessment Procedures Version 3.2.1.
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf, 2018.

M.K. Pratt.
Top 10 in-demand cybersecurity skills for 2021.
https://www.csoonline.com/article/3599095/top-10-in-demand-cybersecurity-skills-for-2021.html, 2020.