CM22014 – Cybersecurity

Coursework: Payment Card Exercise

Professor James Davenport

Set: Monday 03/02/2025 (week 1 of this module) **Due: A) Friday 14/03/2025 (week 6 of this module), 20:00pm** **B) Friday 04/04/2025 (week 9 of this module), 20:00pm** **C) Friday 02/05/2025 (week 11 of this module), 20:00pm**
Percentage of overall unit mark: 60% (0%/40%/20% for the three parts)
Submission Location: Moodle **Submission Components: Data, Report, Report** **Submission Format: .zip for (Part A); .pdf (Parts B,C)**
Anonymous Marking: No

For CM22014, this assessment involves investigating the cybersecurity of the payment card system: first through making a (notional) purchase, then analysing this, then via a group comparative exercise.

Formative feedback on your work will be offered throughout the duration of the coursework:

- During this exercise I will be available to answer questions and offer guidance. Please note that I will not be able to make decisions on behalf of you or your group about the course of the project. I am there to discuss your ideas and offer advice.
- Use Moodle forums to post general questions or questions specific to your project. The unit convener will respond to these as well as your peers. This way we will create a repository of knowledge that will be available to all.

You will receive **summative feedback** on your work within 3 semester weeks of the submission deadline. The feedback will discuss your performance based on the criteria for marking, including what you did well and how specific sections could have been improved.

For **Generative AI**, in terms of https://teachinghub.bath.ac.uk/guide/genai-assessment-categorisation/ this is a Type B assignment: you may use generative AI (for any part of the coursework), but you should acknowledge its use. If you make significant use of a generative AI output, you should quote that output in a footnote (not counted against word count) in the format "Based on Bing Chat in Creative Mode on 21/Jan/2025 which replied <insert raw response>".

Your work will be checked to ensure that you have not plagiarised. For more information about the plagiarism policy at the University see: https://library.bath.ac.uk/referencing/plagiarism

Remember that published work that you refer to in your report should be clearly referenced in your

text and listed in a bibliography section given at the end of your report. For more information see, https://library.bath.ac.uk/referencing/new-to-referencing

Requests for extensions should be made to the Director of Studies. Lecturer and tutors cannot approve extensions.

Payment Card Exercise

This assignment comes in three parts, each following from the previous. The precise dates and weightings are given on the submission pages for each part. Parts A and B are individual; Part C is a group exercise, done in groups assigned on the basis of the outputs from Part A.

Part A: Individual Data Collection

1) Choose a fake payment card. Note that if you just type in 16 digits as your card number, it is unlikely to be syntactically correct: many sites do give correct card numbers for this purpose, e.g. https://www.freeformatter.com/credit-card-number-generator-validator.html or https://ccardgenerator.com/ .
2) Create a file card.txt containing *all* the personal details from the card generator: card number (PAN), CVV, expiry date, holder's name, address etc.
3) Collecting the data described below as you do, attempt to make a purchase from a site of your choice.
    a. The complete log (HAR file) of the browser from the start of the transaction to the point where the payment is declined. There's a FNU (Feature of Negative Utility) in Chrome (at least v84): if you are working in one tab, with logging on, and get switched to a different tab, the different tab doesn't automatically get logged (whereas an iframe in the same tab should get logged). Beware that this might mean you don't log the critical part. The fix to this is to tick the option "preserve logs". Other browsers may have similar issues.
    b. The actual web page into which you entered the PAN, i.e. after the last digit but before you press enter/move to next field/whatever else moves the process on. You may find it helpful in Part B to record precisely the (computer) time at which you move the process on, and the time at which all the card data is entered.
    c. A screenshot of this page at the same point.
4) Bundle (a), (b), (c) *and* the card.txt file into a single zip, and submit this.
    a. If the file is too big, use Dropbox or some such service for the HAR and submit a text file with the details in the zip file.

Part B: Individual Analysis

Based on the HAR you have captured, answer the following questions.

1) [50% of Part B] With which *sites*, e.g. https://google.com *not* https://google.com/maps, does your browser communicate during the transaction? Are there any that worry you, or whose function you do not understand? Note that protocols other than https might be used, e.g. http or wss. The level of detail I expect depends on the number of sites.
    a. <21 sites. A list of each site and its apparent purpose. The list should be numbered.
    b. 21..50 sites. Either as above or with some grouping, e.g. "10 analytics sites, viz …", but each site should be named.
    c. >50 sites. As either method above, but you can group different sites from the same domain, e.g. "7 sites under stripe.com".

2) [20% of Part B] To which site, or sites, does the *complete* PAN get communicated. State the line(s) in the HAR that evidence this. Note that if the PAN is encrypted, this may require a certain amount of deduction ("educated guesswork"), and the times recorded in A3(b) may be useful here. How is the PAN protected in transit? Was it obvious, from the transaction as you observed it as a purchaser (i.e. *not* using the logs) that your data would go there?
3) [20% of Part B] How dependent is the correct functioning of the process you saw on the correct functioning of the DNS? In particular, could a subverted DNS result in any of
    a. Leakage of the PAN (with or without the CVV)?
    b. Failure of the transaction (no money taken and no goods delivered/service rendered)?
    c. Subversion of the transaction (money is taken, but the goods/services are delivered elsewhere)?
    d. Other malfunction?
4) [10% of Part B] Looking at the HTML etc. you have saved, do you feel confident you know what it is doing with your data? In particular, what did you learn from the logs/HTML that you could not have reasonably deduced as a purchaser with no access to these?

Part C: Group Exercise.

Your company is looking to start a new online shop, and the websites your group has been looking at in Part B are the samples provided by the various potential suppliers (refer to the suppliers by the name of the website). Your group is a group of cybersecurity experts, writing a recommendation to the CISO on the cybersecurity of these sample sites. It should be a strict ranking with no ties, but you can add comments like "2 and 3 were very close", "major gap between 3 and 4".

1) [60% of Part C] Give a brief (1/2 page) cybersecurity analysis of each site, and provide the ranking, with justification based on these analyses.
2) [40% of Part C] Are there any features (cybersecurity or not) that you saw in these sites should be recommended for inclusion (or exclusion), e.g. "aardvark.com would have come higher if it hadn't subcontracted PAN verification to armadillo.br over http".