Introduction to cybersecurity for Generalists

James Davenport

University of Bath

16 May 2019

CM50209: Security and Integrity

- Course is 6 ECTS (12 CATS) credits, in Semester 2
- Available on many MSc (including generalist MSc, and corresponding L7 Degree Apprenticeship), also MComp.
- Been running for many years, but IoC was an opportunity to rethink
- Tried to hire a Teaching Fellow, but failed, so I taught it myself
- Partly based on experience as a Fulbright CyberSecurity Scholar at NYU in 2017

Overview (inherited)

Aims:

1. To develop an understanding of the difficulties of security - everyone wants it but no-one can define it.
2. To develop the ability to analyse the security threats to a proposed design.
3. To develop the ability to propose realistic counter-measures, where available.

Learning Outcomes: After taking this unit, the student should be able to:

1. describe common security models;
2. discuss what it means for a given system to be 'secure';
3. identify security weaknesses in proposed systems.

Assessment (inherited format; own exercises)

50% Individual coursework on own experience of PCI DSS online. Buy from three different online vendors: capture both the HTML and the wire data, and analyse for weaknesses.

30% Group coursework: pick an OWASP weakness and give a 30-minute presentation on it.

* Four self-select groups of five — next time I might force groups; not sure how this one will work with Degree Apprentices.

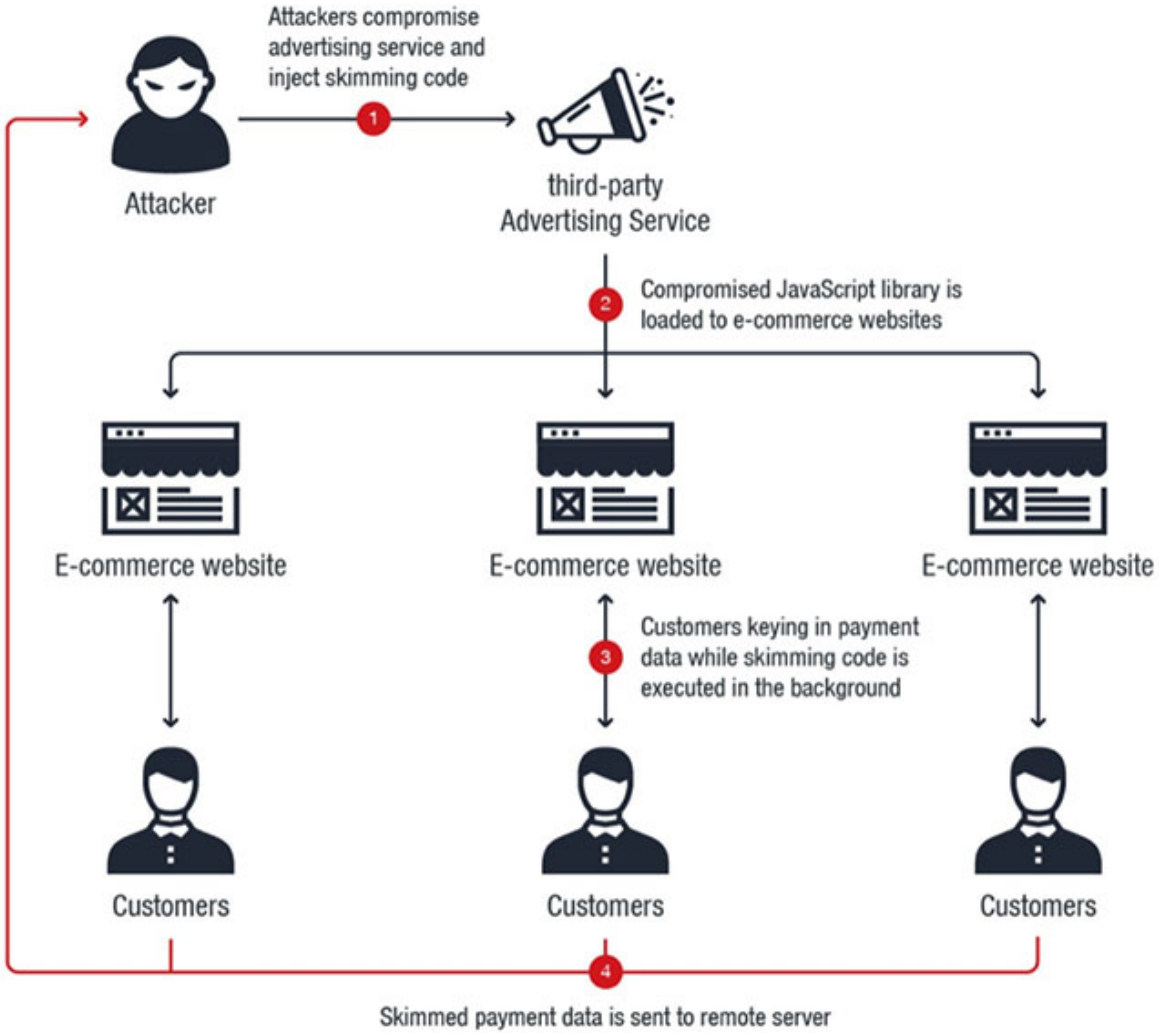
20% Class text (essentially an examination)

Course Overview (12 teaching weeks) I

1. Introduction, resources [And08], CIA triangle. But "In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved. [ISO18]." Proven security [Pau99] but problems with "Plan B" procedures [Com14, "POODLE"].

Course Overview (12 teaching weeks) II

1b Payment Card System: [UK 19a]. Scale of system. The Adverline attack [Zor19, Kli19]



Course Overview (12 teaching weeks) III

2. Cryptography for Security Engineers. Kerckhoffs' Principle [Ker83]. Don't "roll your own".
3. PCI DSS [Pay18b, Pay18a]. Hosted compliance [UK 19b].
4. SQL Injection (example of OWASP for CW2). Lack of understanding [TS19]. Students work on capturing their own PCI DSS data for CW1.
5. Passwords: attacks, salt [MT79], policies, secure storage. Difficulty of correct implementation [NDTS18]. 2FA. Biometrics: weaknesses in practice [RMR17, BRT+17].
6. Access controls (Unix permissions, ACL, setuid, etc.). Principle of least privilege.
7. Vulnerability Scans versus Penetration Testing. PenTest tools [Gri19]. Guest lecture: automobile security.
8. "Consolidation week": no new material.

Course Overview (12 teaching weeks) IV

9. Forensics Principles, ACPO "guidelines" [Ass12]. Importance of ISMS [ISO18] and SIEM. Norsk Hydro as a current example [Clu19, Mun19]. Cyberinsurance, analogy with London Fire Brigade.
10. Guest Lecture (a CISO). Also two group presentations.
11. CSRF (prevented by Token-Based Mitigation, implemented by frameworks); XSS (destroys TBM protection). See `https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.md`. Also two group presentations.
12. Revision and Class Test.

References I


R.J. Anderson.
Security Engineering: A Guide to Building Dependable Cryptosystems (second edition).
Wiley, 2008.


Association of Chief Police Officers.
ACPO Good Practice Guide for Digital Evidence (version 5, October 2011).
ACPO, 2012.


P. Bontrager, A. Roy, J. Togelius, N. Memon, and A. Ross.
DeepMasterPrint: Fingerprint Spoofing via Latent Variable Evolution.
`https://arxiv.org/abs/1705.07386`, 2017.

References II

G. Cluley.
In its ransomware response, Norsk Hydro is an example for us all.
https://www.grahamcluley.com/in-its-ransomware-response-norsk-hydro-is-an-example-f
2019.

Computer Emergency Response Team.
Alert (TA14-290A) SSL 3.0 Protocol Vulnerability and POODLE Attack.
https://www.us-cert.gov/ncas/alerts/TA14-290A,
2014.

References III

R.A. Grimes.
Penetration testing on the cheap and not so cheap.
https://www.csoonline.com/article/2622078/hacking-penetration-testing-on-the-cheap-and-not-so-ch
html, 2019.

ISO/IEC.
ISO/IEC 27000:2018 (E): Information technology - Security techniques - Information security management systems - Overview and vocabulary.
https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip, 2018.

References IV

A. Kerckhoffs.
La cryptographie militaire.
Journal des sciences militaires, 9:5–38, 1883.
URL: http://www.petitcolas.net/kerckhoffs/crypto_militaire_1.pdf.

Y. Klijnsma.
New Year, Same Magecart: The Continuation of Web-based Supply Chain Attacks.
https://www.riskiq.com/blog/labs/magecart-adverline/, 2019.

References V


Robert Morris and Ken Thompson.
Password security: A case history.
Commun. ACM, 22(11):594–597, November 1979.
URL: http://doi.acm.org/10.1145/359168.359172,
doi:10.1145/359168.359172.


P. Muncaster.
Norsk Hydro Admits Ransomware Costs May Have Hit $41m.
https://www.infosecurity-magazine.com/news/norsk-hydro-ransomware-costs-hit-1-1/, 2019.


A. Naiakshina, A. Danilova, C. Tiefenau, and M. Smith.
Deception Task Design in Developer Password Studies: Exploring a Student Sample.
In Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018). USENIX Association, pages 297–313, 2018.

References VI


L.C. Paulson.
Inductive Analysis of the Internet Protocol TLS.
ACM Trans. Information and System Security, 2:332–351, 1999.


Payment Card Industry Security Standards Council (PCI SSC).
PCI DSS Quick Reference Guide.
https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf, 2018.


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.

References VII


A. Roy, N. Memon, and A. Ross.
MasterPrint: Exploring the Vulnerability of Partial Fingerprint-based Authentication Systems.
IEEE Transactions on Information Forensics and Security, 12:2013–2025, 2017.


C. Taylor and S. Sakharkar.
');DROP TABLE textbooks;–: An Argument for SQL Injection Coverage in Database Textbooks.
In Proceedings of the 50th ACM Technical Symposium on Computer Science Education (SIGCSE '19). ACM, pages 191–197, 2019.


UK Finance.
Card Payment Cycle.
http://www.theukcardsassociation.org.uk/getting_started/card-payment-cycle.asp, 2019.

References VIII

UK Finance.
How to be PCIDSS Compliant.
http://www.theukcardsassociation.org.uk/security/how_to_be_PCIDSS_compliant.asp, 2019.

Z. Zorz.
Compromised ad company serves Magecart skimming code to hundreds of websites.
https://www.helpnetsecurity.com/2019/01/17/magecart-supply-chain-attack/, 2019.