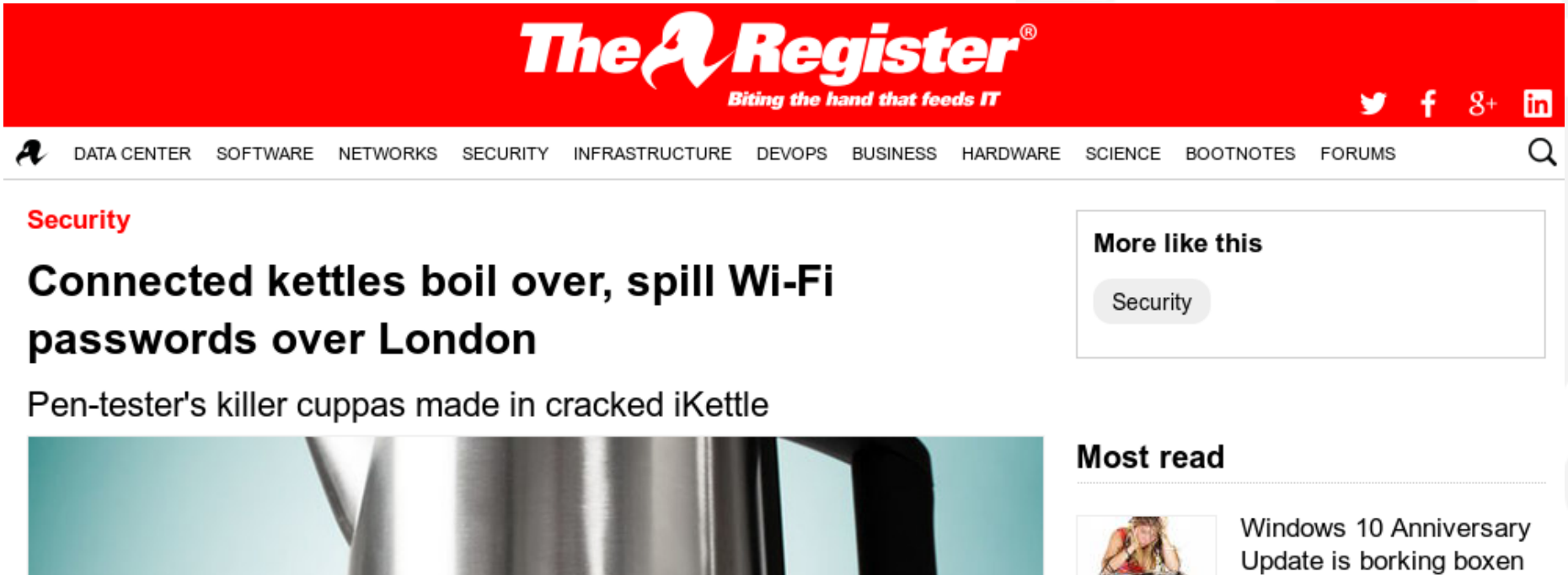
Learning From Others' Mistakes:
Penetration Testing IoT Devices in the Classroom

Tom Chothia and **Joeri de Ruiter**

Penetration testing course

- Masters course
- Taught at University of Birmingham, UK
- Two practical assignments
  - Analysing commercial off-the-shelf IoT devices



Learning objectives

- Collect and analyse network traffic
- Understand commonly used network protocols
- Simple reverse engineering of code
- Perform penetration tests of IoT devices
- Present results of a penetration test in form of a report and presentation

Introduction

- Introduction to penetration testing
- Relevant standards (e.g. PCI-DSS, NIST SP800-115)
- Legal and ethical issues

Analysing network traffic

- Web security
  - Common attacks: SQLi, XSS, CSRF
  - Burp Proxy to intercept, view and alter web traffic
  - Practical exercise with VM running vulnerable web application
- Network protocols
  - HTTP and TLS
  - Network scanning with Nmap
  - Capturing of network traffic using Wireshark
  - TLS man-in-the-middle using Burp Proxy

Reverse engineering

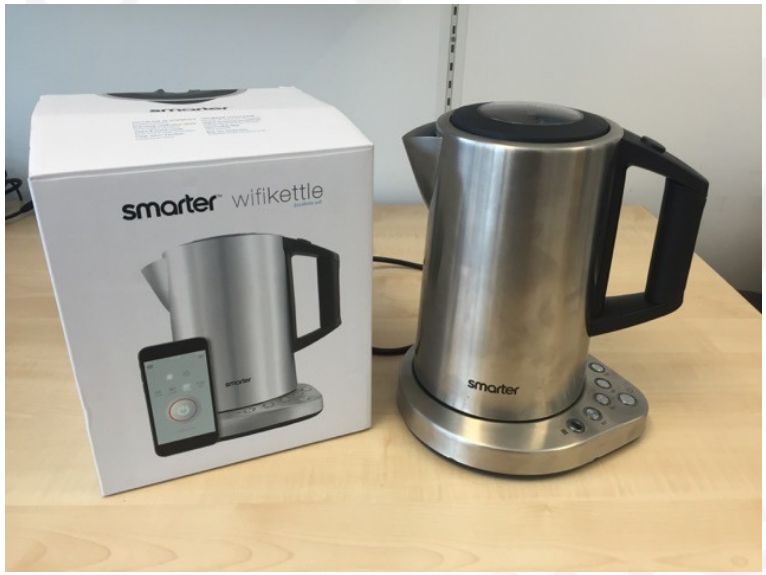
- Android / Java apps
  - Apktool, dex2jar and JD-GUI tools introduced
  - Tools useful for group assignment
- x86 binaries
  - IDA Pro
  - Buffer overflows
- Practical exercise on buffer overflows

Practical assignments

- Analysis of commercial off-the-shelf IoT devices
- Results in report and presentation
- Students signed declaration
  - Only analysis of device and app, no backends
  - No publicity without permission from staff

First group assignment

- Analysis of vulnerable IoT device
- Groups of 4
- Lasted for 4 weeks
- Individual group meetings to discuss progress
- Lab session to get help with the tools



Vulnerable devices

- Easy to find vulnerabilities
  - Known vulnerabilities
  - Found during quick manual analysis
- Can be during setup
  - For example, sending Wi-Fi credentials over unprotected Wi-Fi connection
- Or when device is used
  - For example, improper use of TLS

Results first assignment

- All groups found some vulnerability
- Findings were presented to class
  - Demos given of found attacks
- Reports were peer reviewed by students

Student reviews

- Reports of first assignments were reviewed and ranked by all students
  - One paragraph per reviewed report
- Not taken into account for grade of reviewed report
- Review reports were part of the final grade
- Useful exercise for the students

Second group assignment

- Different groups
  - Knowledge sharing
- Unknown whether devices were vulnerable
- Less guidance
- Grade based on report
  - Finding vulnerability not necessary for good grade

Results second assignment

- New vulnerabilities found
  - Home alarm system: app used same credentials over TLS and plaintext connection
  - Smart padlock: validity period only checked by app and master code provided to guest users
  - Smart camera: face recognition fooled using Facebook pictures
- Knowledge shared after first exercise

Grading

- Practical assignments
  - Analysis of device functionality (25%)
  - Risk analysis (10%)
  - Substantialness of achievement (15%)
  - Report (20%)
  - Presentation (20%)
  - Teamwork (10%)

Grading

- Final grade
  - Written exercises (10%)
  - First practical assignment (40%)
  - Peer reviews (10%)
  - Second practical assignment (40%)
- No students failed
- Distribution of marks comparable to other courses

Student feedback

- Course very well received
- Maximum score for
  - How worthwhile course was
  - The amount learned
  - How interesting course was
- Rated slightly harder than average
- Practical aspects, learned skills and use of real IoT devices especially appreciated
- Students would have liked more time for analysis

Conclusions

- IoT devices provide good learning material to teach penetration testing techniques
  - All groups found vulnerabilities
- Having two rounds improved knowledge sharing
  - First round builds confidence that the students can find vulnerabilities
- Course very well received by the students

Thanks for your attention!

Teaching material available on:
http://www.cs.bham.ac.uk/~tpc/Edu/Pentesting/