Imperial College
London

446H – Applied Network Security

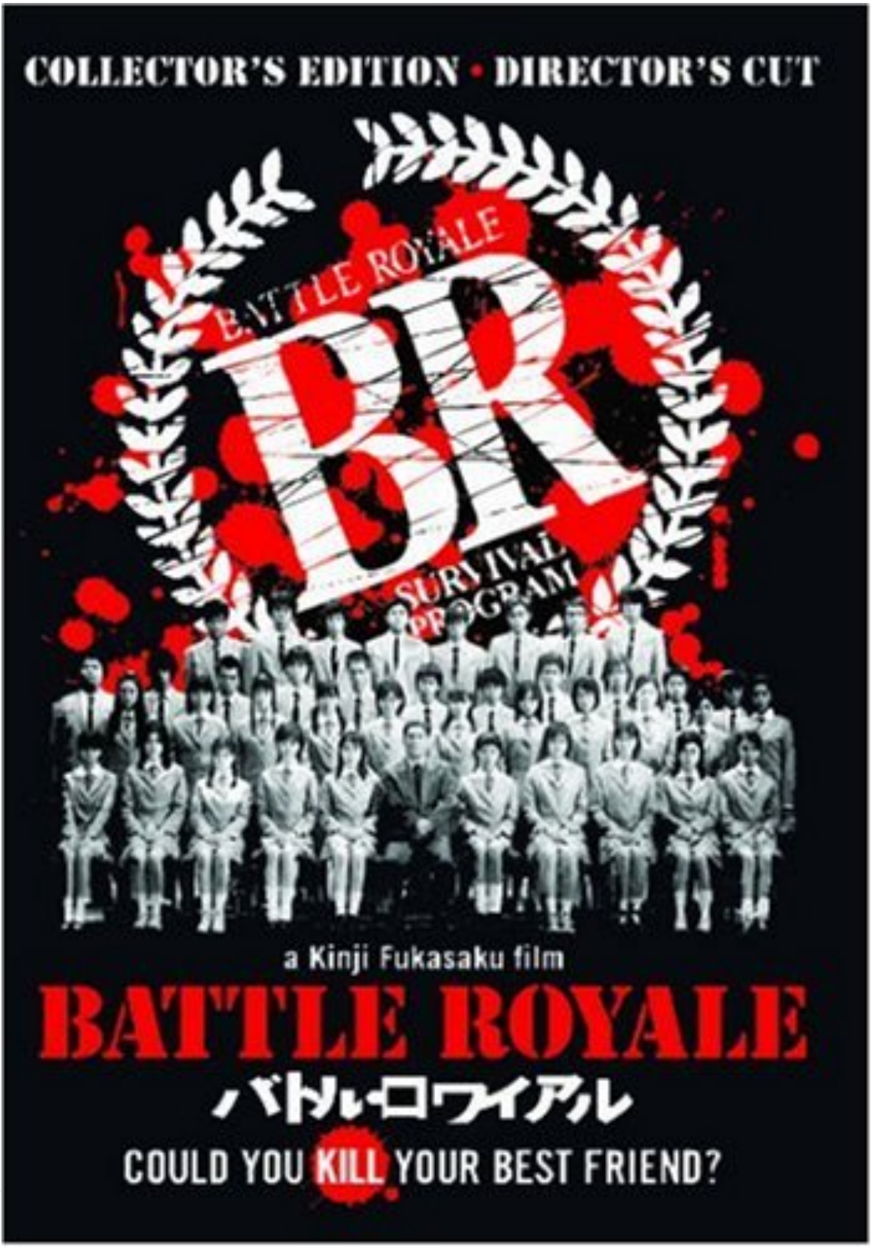
4. WiFi security

Dr Sergio Maffeis
Department of Computing
Course web page: https://446h.cybersec.fun

Project 4

Imperial College London

- **WiFi Battle Royale**
  - Goal: attack and defend WiFi networks
- Part 1: CTF
  - In H308, 2pm-4pm, on 8/3
- Part 2: Preparation
  - What are the threats to WiFi networks?
  - How do attackers pwn networks, what tools do they use?
- Scope
  - Common configurations of IEEE 802.11 a/b/g/n networks
  - Supporting a combination of open access, WEP, WPA, WPA2 (including Enterprise), and optionally WPA3.
    - No Enterprise, WPA3 for part 1
  - Other networks or configurations are not in scope.



Battle Royale

- You will gain points by reporting flags corresponding to the solution of challenges.
- Flag submissions will also be over WiFi networks that are part of the CTF, so it is acceptable, and in fact encouraged, to "steal" flags from other groups (you will be awarded points for this, even for tasks you have solved already).
- The less flag will be reported by the other groups, the more valuable yours will be: you are allowed to disrupt attempts of other groups to capture the flags, and you are encouraged to defend yourself from disruption.

Warnings

- All the SSID of networks created for the CTF (including any hidden SSID if any) **will** begin with the string "446HCTF".
- The (public or hidden) SSID of any network that you may decide to create **must** begin with the string "446HCTF".
- You **must not** sniff the traffic of any network not related to the CTF.
- You **must not** inject traffic on any network not related to the CTF, and if you are detected doing so (even unintentionally) your participation to the CTF will be terminated (you will keep flags obtained up to that point).

Preparation

- During the CTF you will be asked to run an access point
  - providing access to a web page you serve on a local network under your control
  - that the lecturer should be able to access from a standard Web browser via a standard WiFi client.
- You are advised to prepare this infrastructure in advance.
  - You may want to implement protections against unauthorised access to the web page by other groups
  - you cannot ask the lecturer to anything more that using a network key or username/passwords you provide
  - for example using application-level end-to-end encryption is out of scope

Report

- The report should be between 5 pages in length.
- Page 1: threat analysis for a residential Wifi (base it on the setup of the home network of one of the members of your group, feel free to "anonymise" if you want).
- Page 2: threat analysis for a free WiFi in a coffee shop or similar (be real, pick one, analyse it).
- Page 3: threat analysis for the "Imperial" WiFi available on campus (not Imperial WPA).
- Pages 4-5: summarise your TTPs research.