Risk assessment for

Network Scanning/Security Vulnerability research

Date submitted:

Principal investigator: Christopher Hargreaves

Other Oxford University researchers/students/staff involved: Tian Guo (Deon)

Contact email: deon.guo@gmail.com

Others involved in carrying out the research (e.g. researchers at other institutions):

Will this research be funded? No

Funder:

Grant reference number (if available):

Project name (if this study is part of a larger project):

Title of this study: Attacking Home Wifi Network with Kali

Anticipated start/end dates: 01/04/2021 - 01/09/2021

1. **Brief overview of your study**

*What are you investigating, and why? How will you do it?*

The wireless wifi network is an essential part of almost every home, especially nowadays when working from home is becoming a necessity and as more and more IoT devices join our home.

With most ISPs, the wifi router comes pre configured and is usually ‘plug and play’. The simplistic architecture and topology gives great convenience for the users as any device can simply join the wifi with a passphrase. The home wifi setup generally does not include any further security considerations as most occupants do not have the awareness, expertise and adequate tools.

On the other hand, the rise of open-source penetration testing automation tool sets, represented by Kali Linux, have made hacking accessible and easy for anyone with access to the internet.

So how secure is our home wifi network against Kali? In this project we investigate the vulnerabilities and their impact of typical home wifi networks. More specifically, we perform penetration tests on such a network as a case study to assess if and how a home wifi network’s confidentiality, integrity, availability and privacy can be compromised by Kali.

1. **Do you anticipate any possibility of encountering personal data in this research, or of using human participants (even incidentally)?**

*If Yes – please submit a CUREC-1A checklist form (guidance specific to the Computer Science Department* [*here*](https://intranet.cs.ox.ac.uk/research-ethics/)*)*

No

1. **List all the possible negative risks/outcomes that might arise if the research is successful.**

*For reach risk/outcome state how likely this is to occur and what steps will be taken to avoid or mitigate it. You are required to cover all relevant perspectives and include unlikely risks if they have the potential to be very harmful. However, you can also be pragmatic and realistic in your assessment.*

|  |  |  |
| --- | --- | --- |
| *Potential risk* | *Likelihood* | *Mitigation* |
| uninvited devices join the experiment network | low | set up the wifi network away from public space  require authentication whenever possible  router stays offline when password is weak  router turned off when not in use  monitor the network and block uninvited devices |
| captured neighboring wifi network's traffic | low | set up the wifi network in a remote location, further from other households  parameterise scans base on wifi ID  only connect to our experiment wifi network |
| exploits persistent even after experiments completed | low | reinstall systems upon experiment completion  factory reset devices upon experiment completion |
| test data sent to service provider online | medium | keep the network disconnected from the internet whenever possible  use non-sensitive data when generating test data |

1. **Explain why you feel the research is desirable in the light of those risks.**

First of all, the impact and likelihood of all the risks are reasonably low. They will by no means cause any significant damage to any participants or organisation. We have taken ethics considerations to design the research in such a way most of the ethics risks are mitigated, i.e., we will create our own test network and simulate test data to conduct experiments with.

On the other hand, the research will provide important insight in helping protect ordinary families from various attacks, a desirable contribution.

1. **Describe your responsible disclosure strategy.**

*How do you plan to report/publicise your findings, e.g. working with appropriate companies/vendors to report security weaknesses, delaying such publication until they’ve been given sufficient time to fix problems, etc.*

Should any defect or security issues be discovered with any devices included in the research, we will follow the vendor’s disclosure policy published on their website. If there is none, we will contact the vendor via email and work with them for a responsible disclosure strategy agreed by both parties.

1. **In which legal jurisdiction(s) will the research take place?**

New Zealand and UK

1. **What are the legal issues which could arise in the conduct of the research, in that (those) jurisdictions?**

*These might include: UK* [*Computer Misuse Act*](https://www.legislation.gov.uk/ukpga/1990/18/contents)*,* [*Wireless Telegraphy Act 2006*](https://www.legislation.gov.uk/ukpga/2006/36/contents)*,* [*Investigatory Powers Act 2016*](https://www.legislation.gov.uk/ukpga/2016/25/contents)*; USA* [*Computer Fraud and Abuse Act*](https://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act)*,* [*Digital Millennium Copyright Act*](https://www.law.cornell.edu/uscode/text/17/1201)*, etc. Oxford University Legal Services may be consulted for a further view on these questions.*

UK: Computer Misuse Act

New Zealand: Crimes Bill 1989

1. **Might your work fall under the** [**UK strategic export control lists**](https://www.gov.uk/guidance/export-military-or-dual-use-goods-services-or-technology-special-rules)**?**

*The UK strategic export control lists cover items, systems, raw materials and components designed or modified for military use, or which could be used for both military and civilian purposes.* [*Full lists here*](https://www.gov.uk/government/publications/uk-strategic-export-control-lists-the-consolidated-list-of-strategic-military-and-dual-use-items-that-require-export-authorisation)*.*

no

1. **What contractual issues may arise?**

*E.g. from software licencing (have you/the university signed anything to say you will not reverse engineer something) or from copyright infringement.*

I will not reverse engineer anything or infringe copyright

1. **If this research is successful, how might this vulnerability be used by malicious actors?**

*You can refer to the risk/mitigation table above; see the EC’s H2020* [*How to complete your ethics self-assessment*](http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf) *for useful guidance on misuse of research results.*

The penetration techniques being used in this project are all known and documented. We do not expect to discover any new techniques that may be used by malicious actors.

1. **What risks are there to the researcher(s),**

**(a) in the conduct of the experiments,**

none

**(b) following disclosure or publication of results?**

none