CSC 15

John Ryan Zelling Analyst

Jan 2017

Contents

CSC 15.0

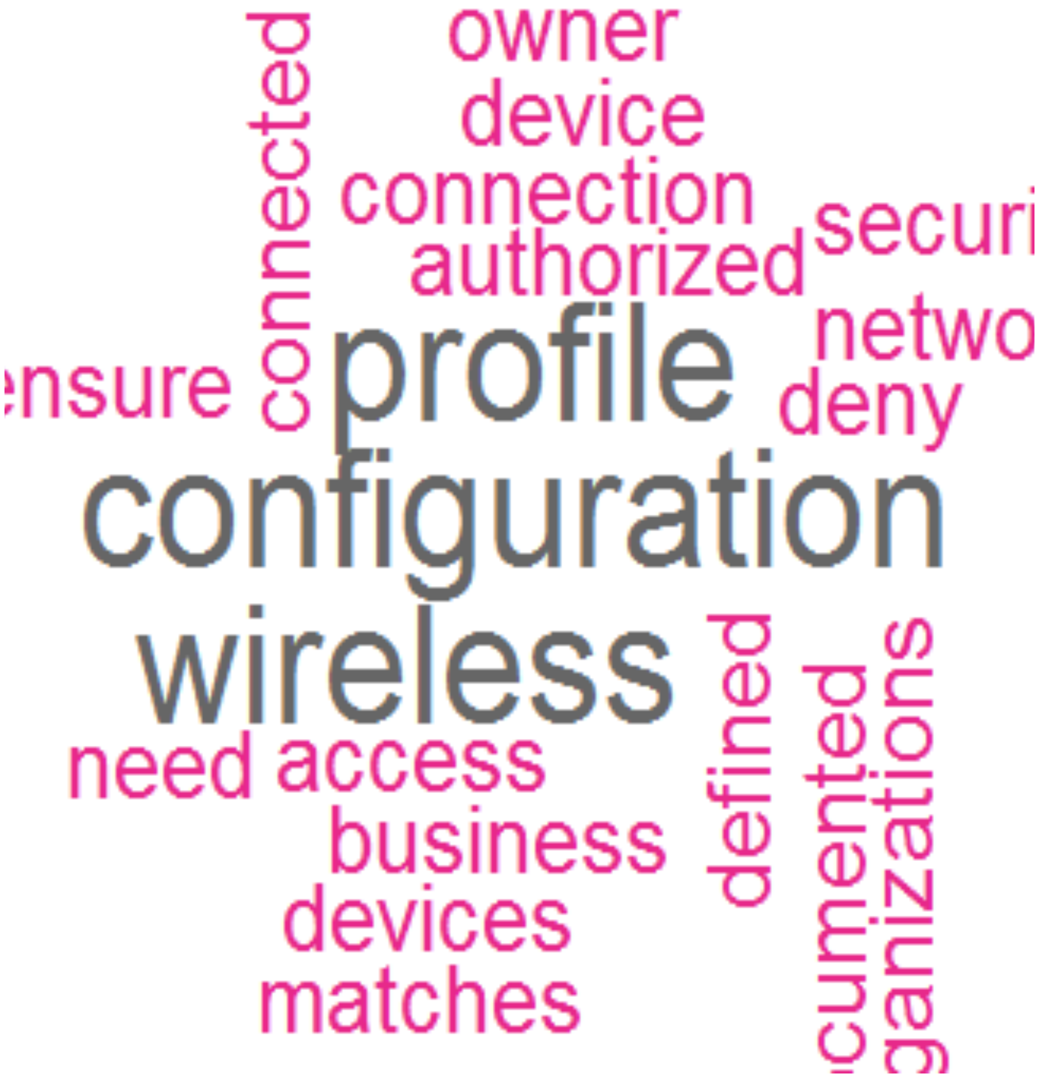
[1] “Critical Security Control #15: Wireless Access Control”

1

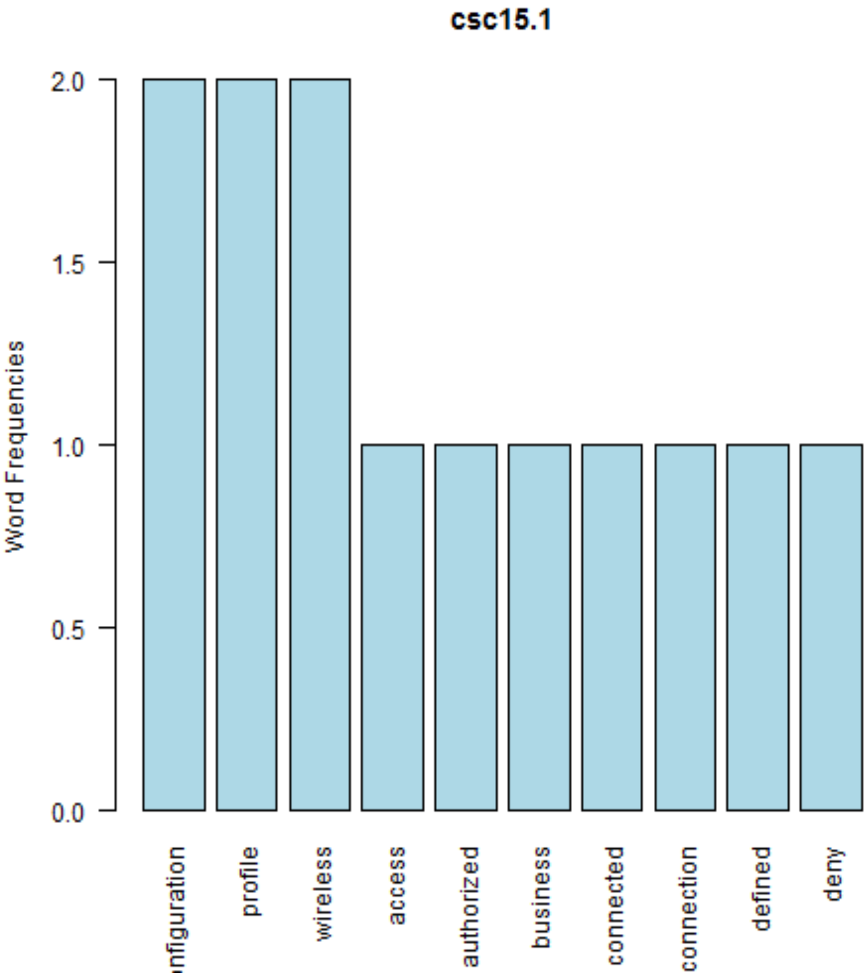
[1] [1] “To further clarify the Creative Commons license related to the CIS Critical Security Controls content, you are authorized to copy and redistribute the content as a framework for use by you, within your organization and outside of your organization for non-commercial purposes only, provided that (i) appropriate credit is given to CIS, and (ii) a link to the license is provided. Â Additionally, if you remix, transform or build upon the CIS Critical Security Controls, you may not distribute the modified materials. Users of the CIS Critical Security Controls framework are also required to refer to (http://www.cisecurity.org/critical-controls.cfm) when referring to the CIS Critical Security ControlsÂ in order to ensure that users are employing the most up to date guidance. Â Commercial use of the CIS Critical Security Controls is subject to the prior approval of The Center for Internet Security.”

CSC 15.1

[1] “configuration + profile”



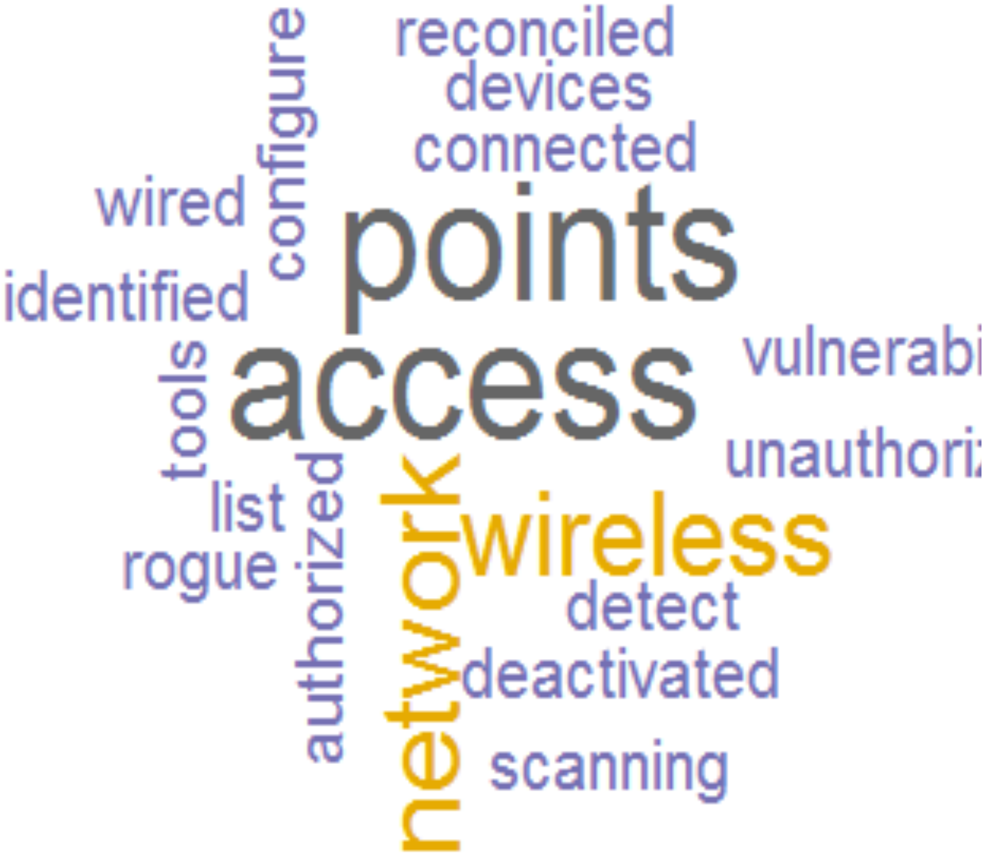
null device 1



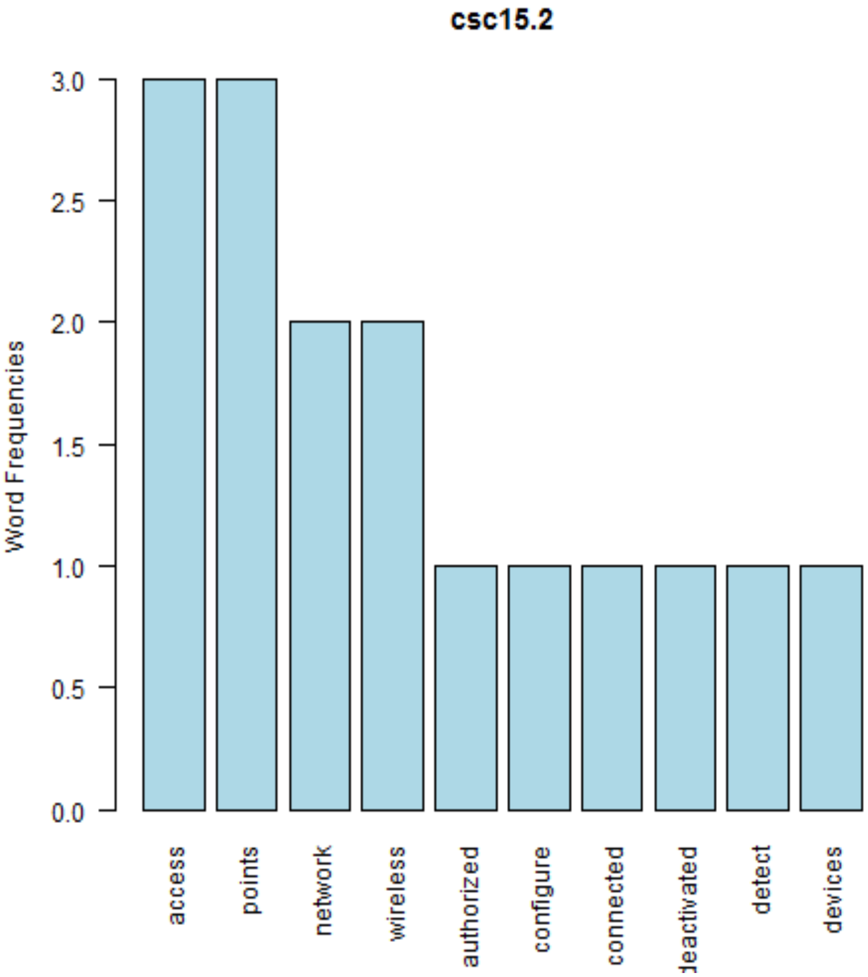
null device 1 [1] “Ensure that each wireless device connected to the network matches an authorized configuration and security profile, with a documented owner of the connection and a defined business need. Organizations should deny access to those wireless devices that do not have such a configuration and profile.”

CSC 15.2

```
[1] “access + points”
```



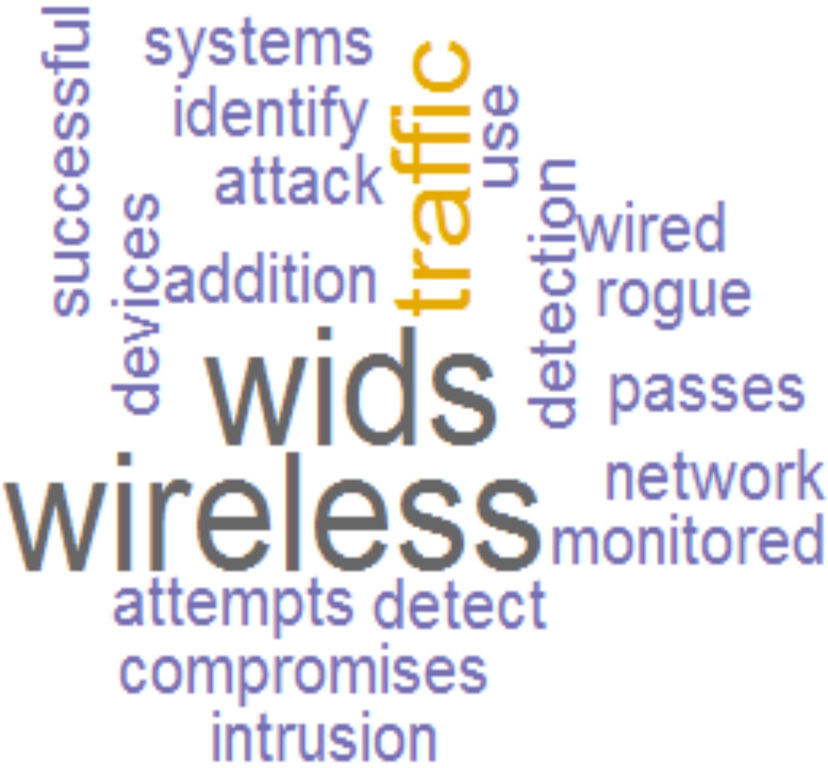
```
null device 1
```



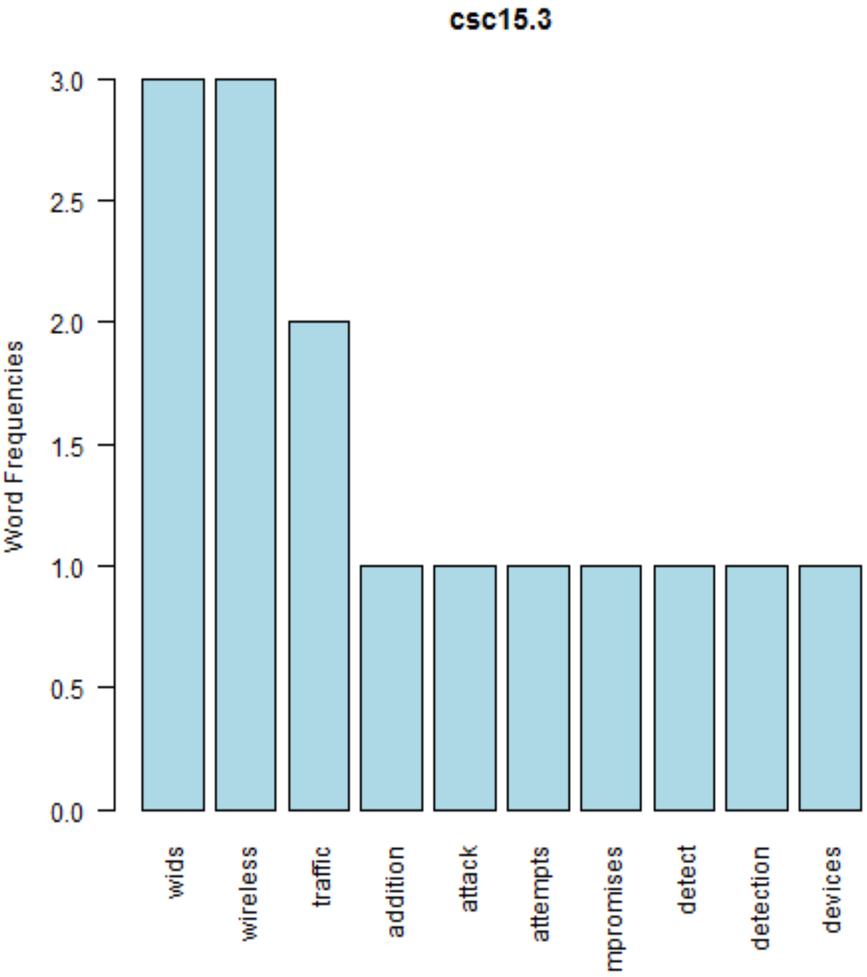
null device 1 [1] "Configure network vulnerability scanning tools to detect wireless access points connected to the wired network. Identified devices should be reconciled against a list of authorized wireless access points. Unauthorized (i.e., rogue) access points should be deactivated."

CSC 15.3

[1] “wids + wireless”



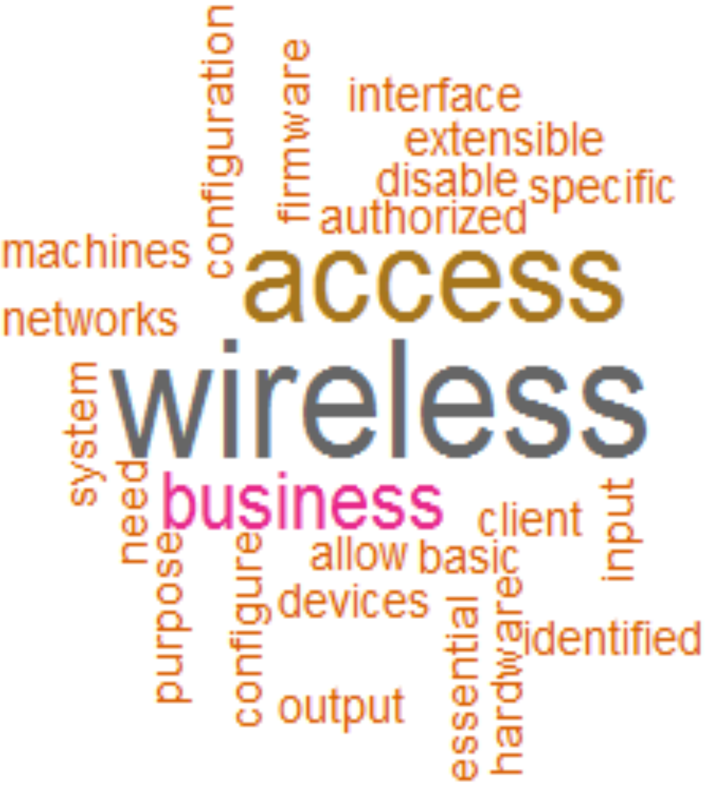
null device 1



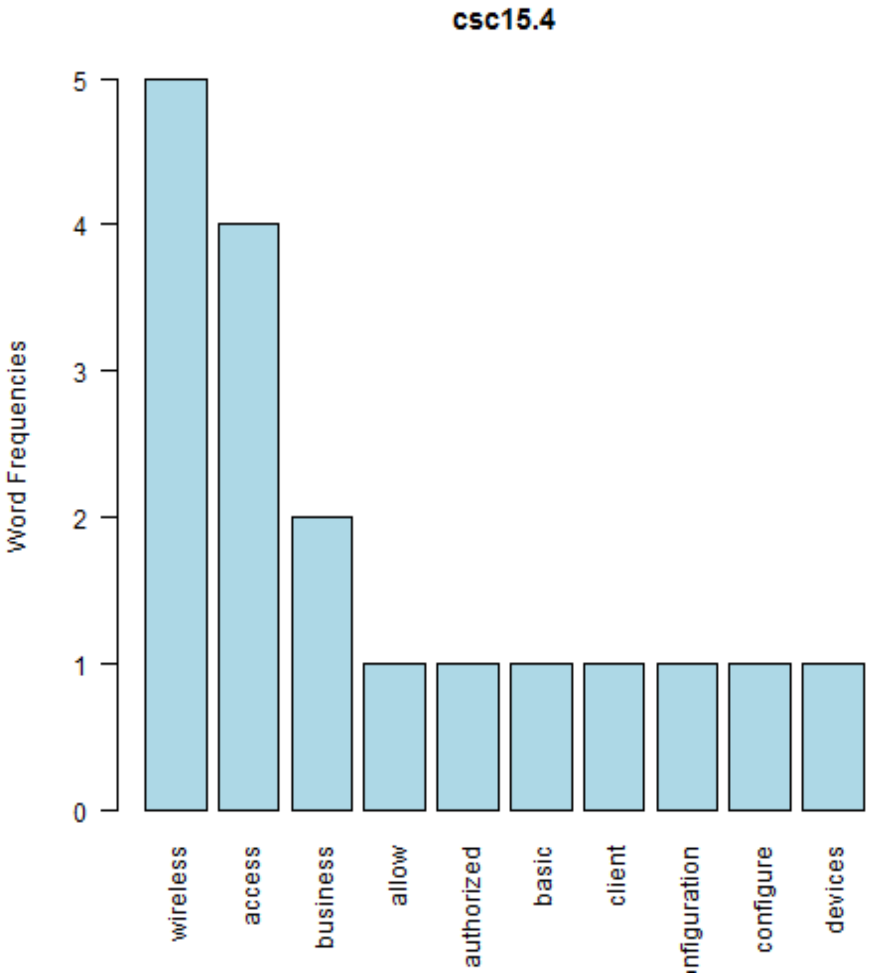
null device 1 [1] “Use wireless intrusion detection systems (WIDS) to identify rogue wireless devices and detect attack attempts and successful compromises. In addition to WIDS, all wireless traffic should be monitored by WIDS as traffic passes into the wired network.”

CSC 15.4

[1] “wireless + access”



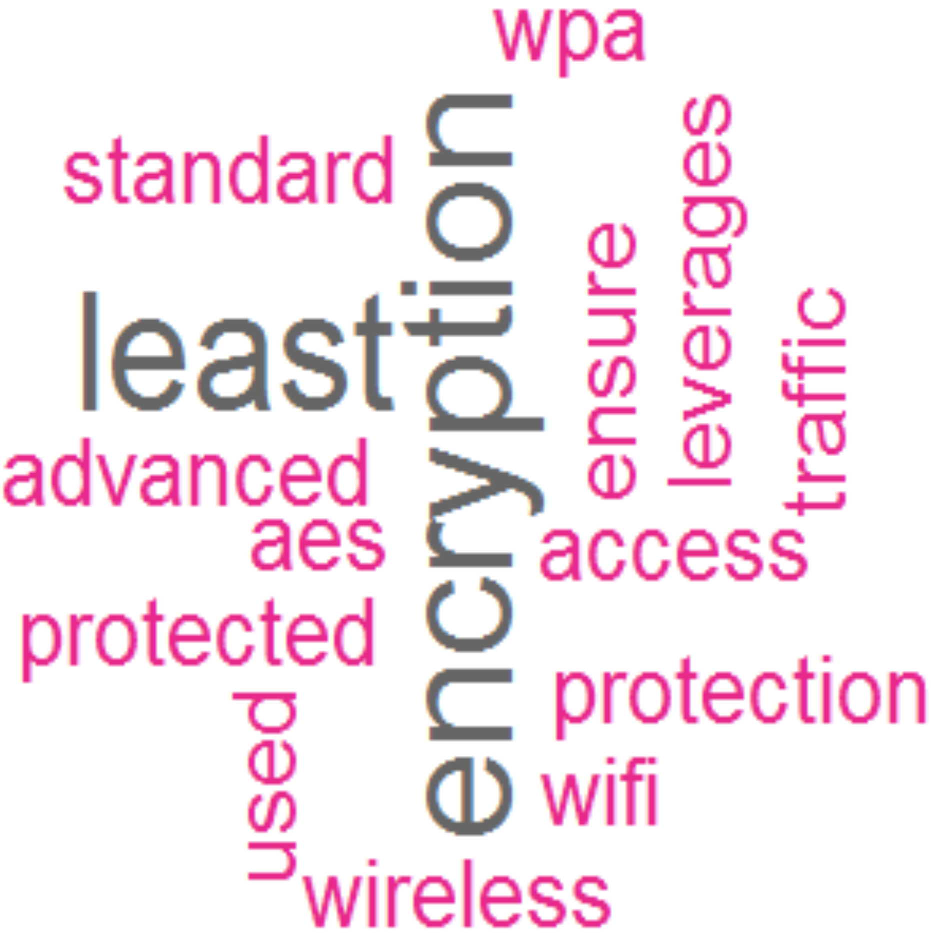
null device 1



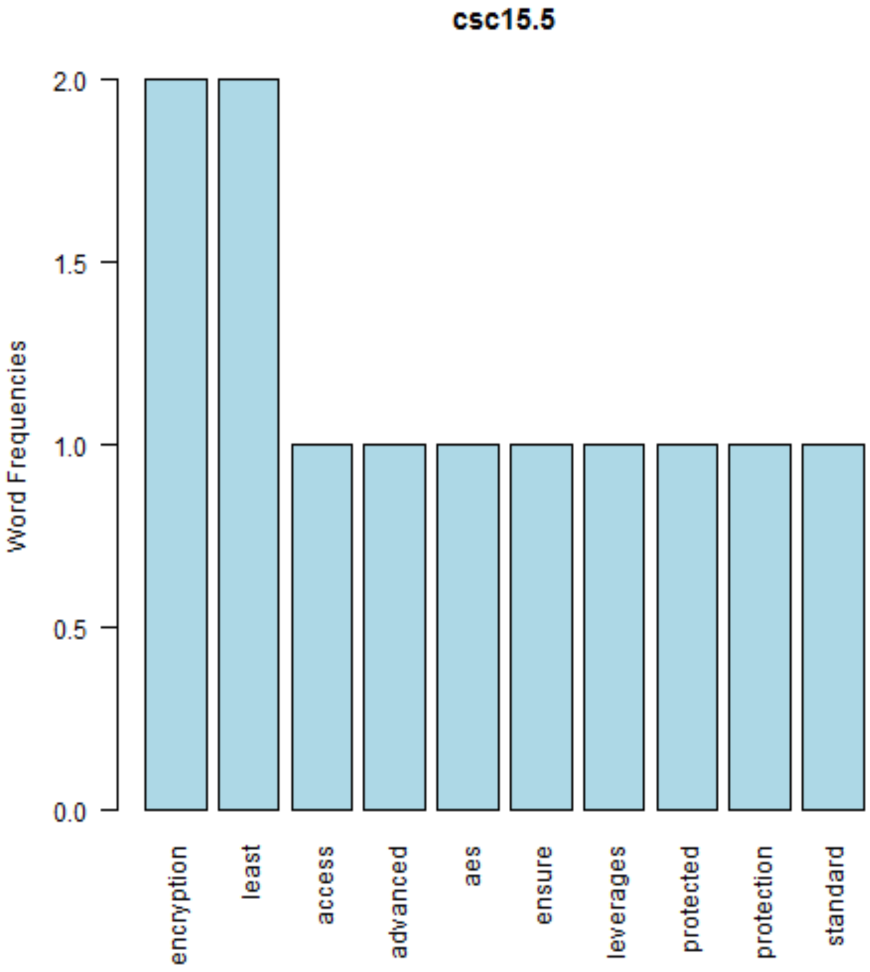
null device 1 [1] “Where a specific business need for wireless access has been identified, configure wireless access on client machines to allow access only to authorized wireless networks. For devices that do not have an essential wireless business purpose, disable wireless access in the hardware configuration (basic input/output system or extensible firmware interface).”

CSC 15.5

[1] “encryption + least”



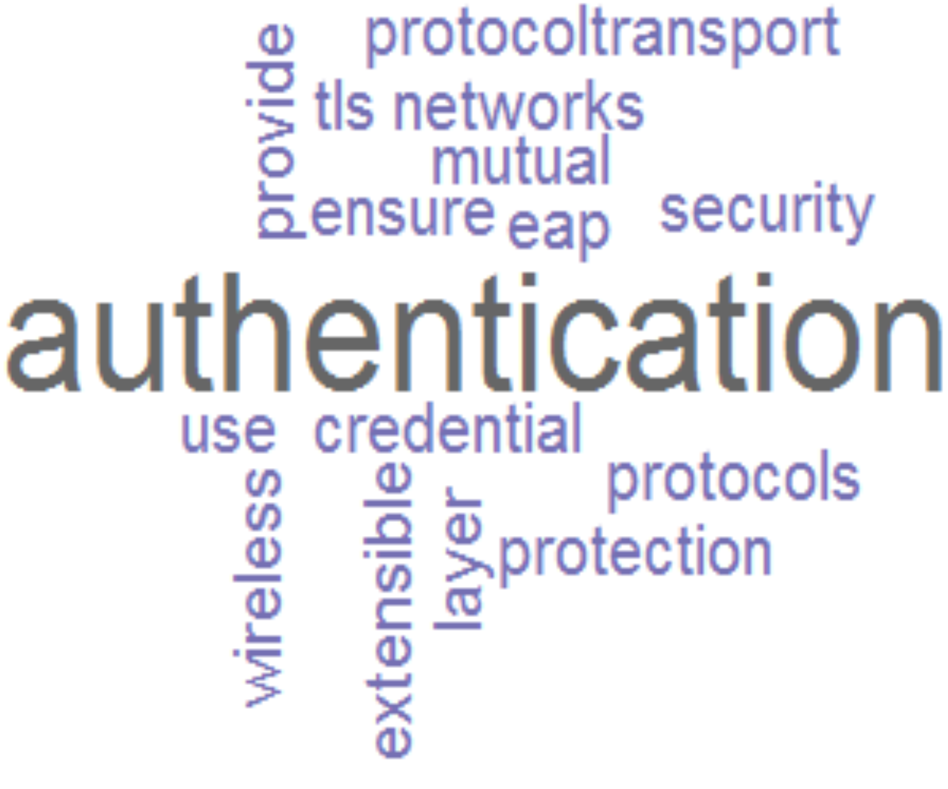
null device 1



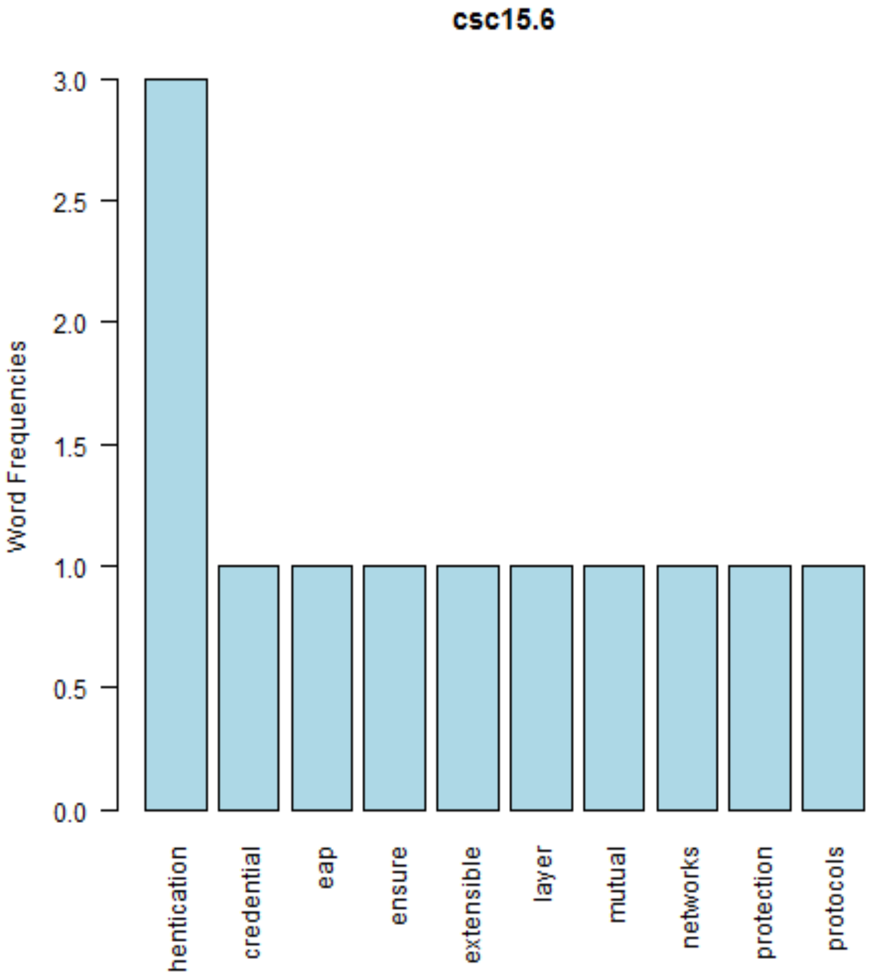
null device 1 [1] “Ensure that all wireless traffic leverages at least Advanced Encryption Standard (AES) encryption used with at least Wi-Fi Protected Access 2 (WPA2) protection.”

CSC 15.6

[1] “authentication + credential”



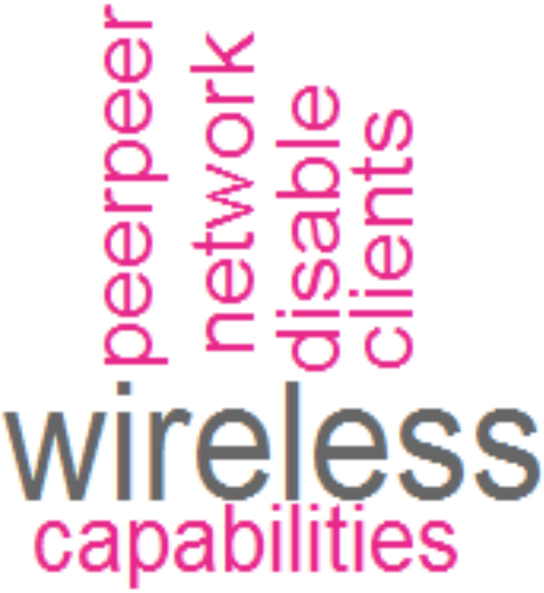
null device 1



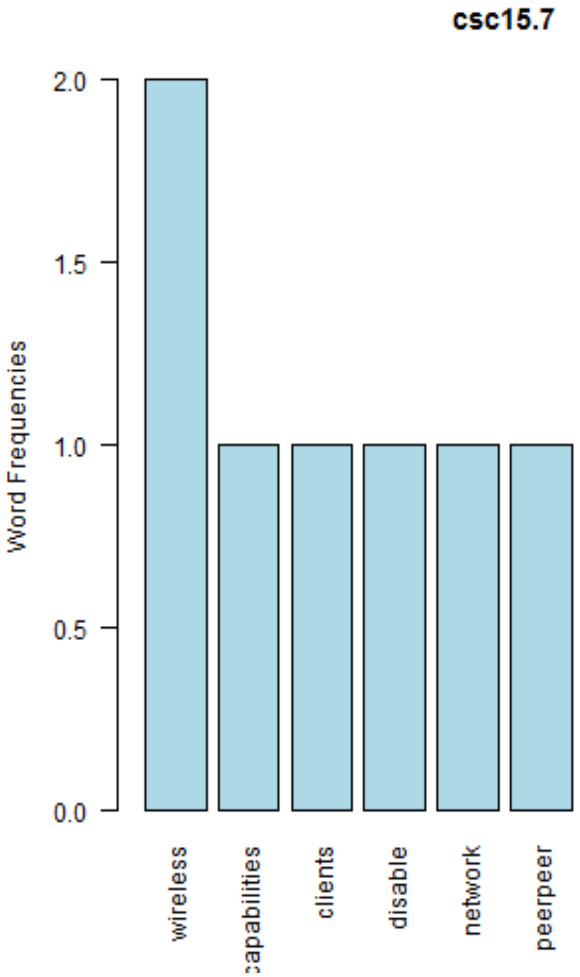
null device 1 [1] “Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), which provide credential protection and mutual authentication.”

CSC 15.7

[1] “wireless + capabilities”



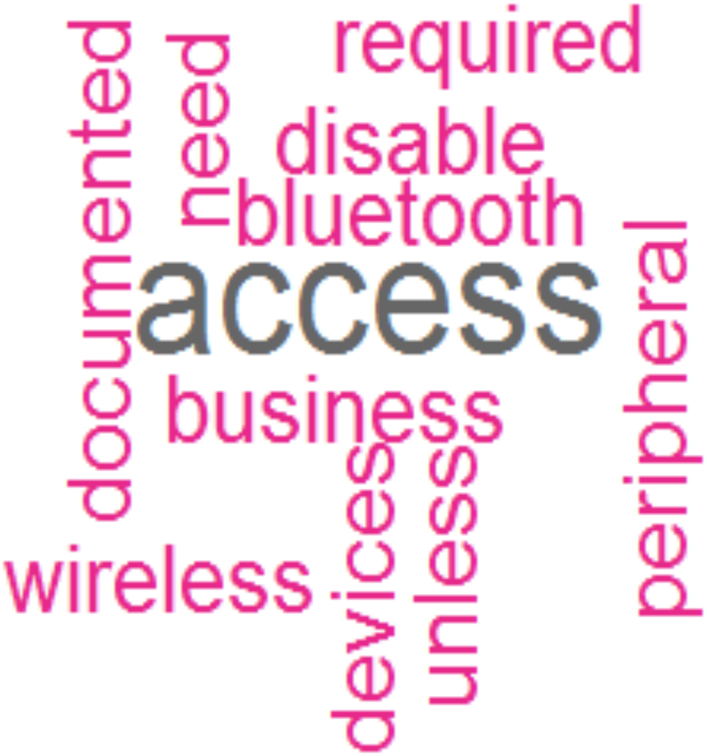
null device 1



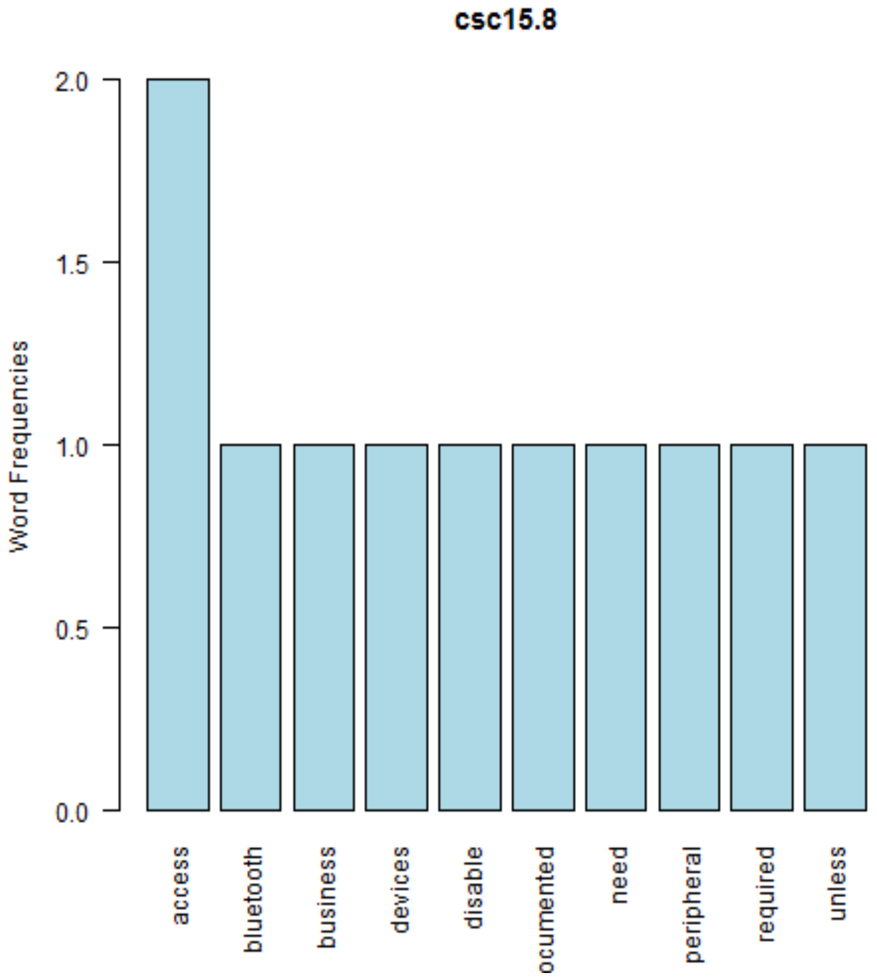
```
null device 1 [1] "Disable peer-to-peer wireless network capabilities on wireless clients."
```

CSC 15.8

```
[1] “access + bluetooth”
```



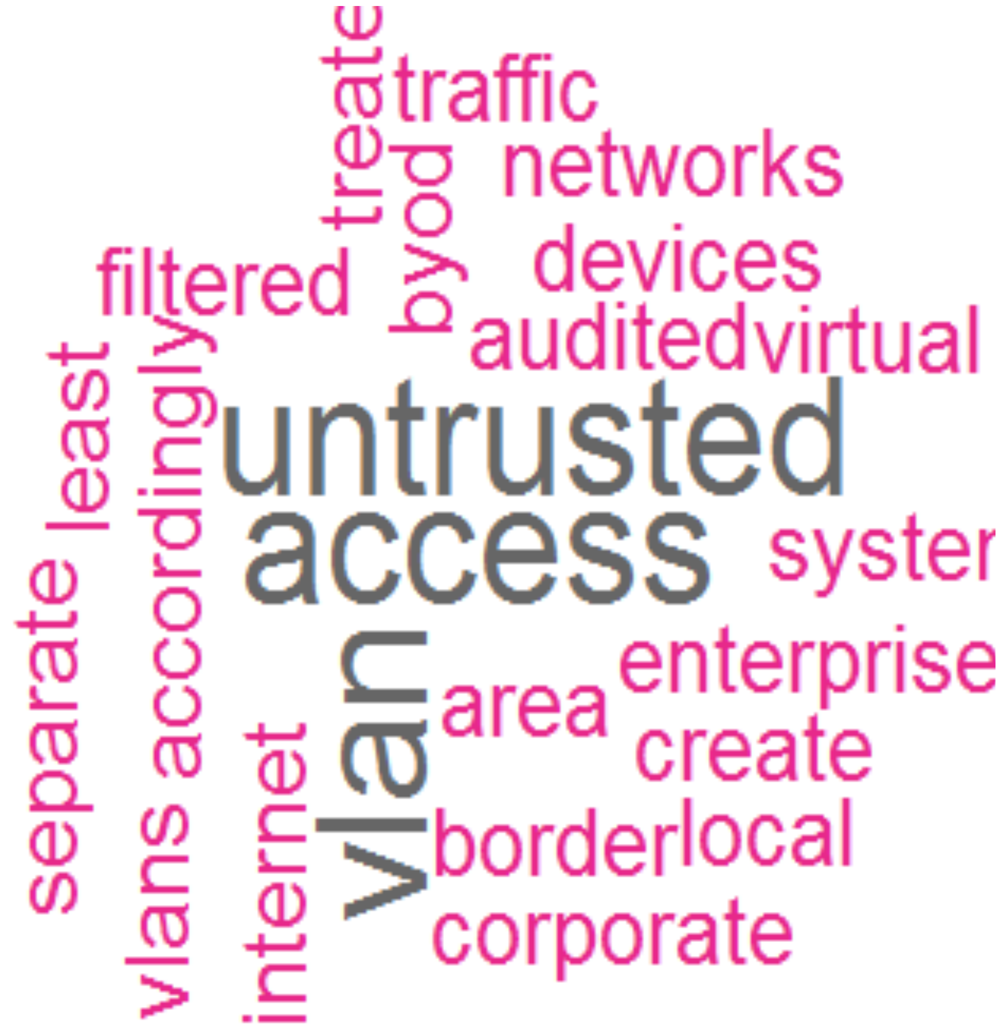
```
null device 1
```



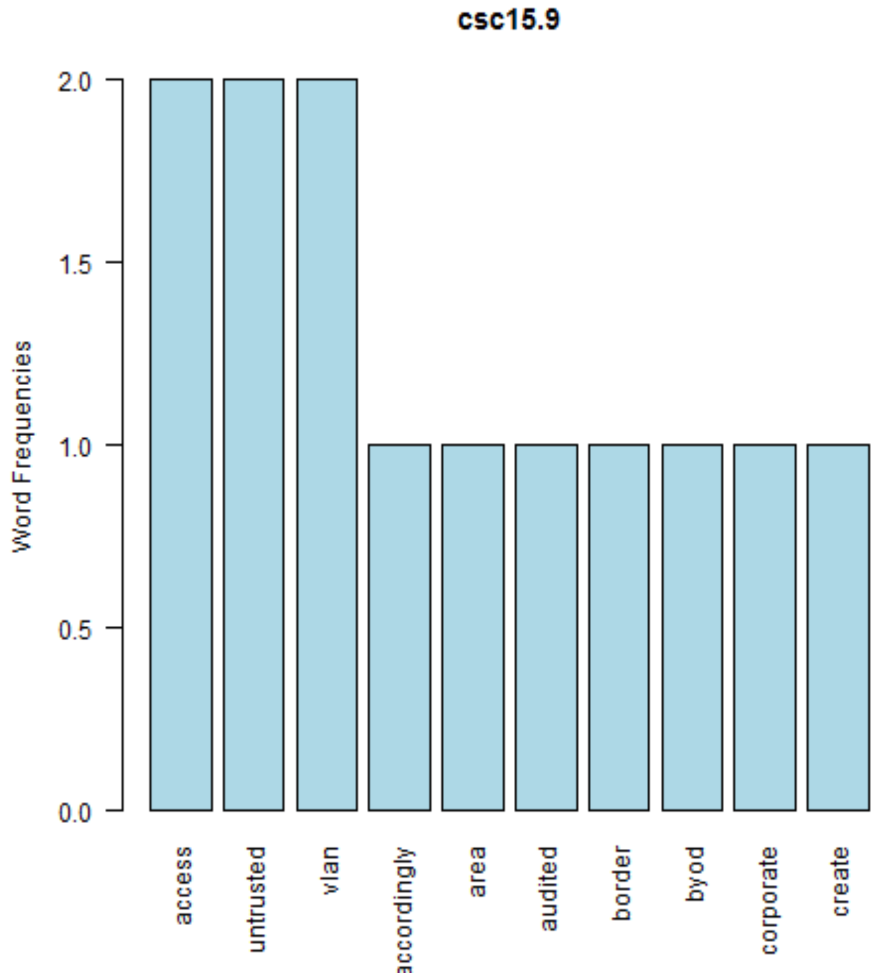
null device 1 [1] “Disable wireless peripheral access of devices (such as Bluetooth), unless such access is required for a documented business need.”

CSC 15.9

[1] “access + untrusted”



null device 1



null device 1 [1] “Create separate virtual local area networks (VLANs) for BYOD systems or other untrusted devices. Internet access from this VLAN should go through at least the same border as corporate traffic. Enterprise access from this VLAN should be treated as untrusted and filtered and audited accordingly.”