University *of Ljubljana*
Faculty of *Computer and Information Science*

Layer 2 user isolation in Eduroam.si

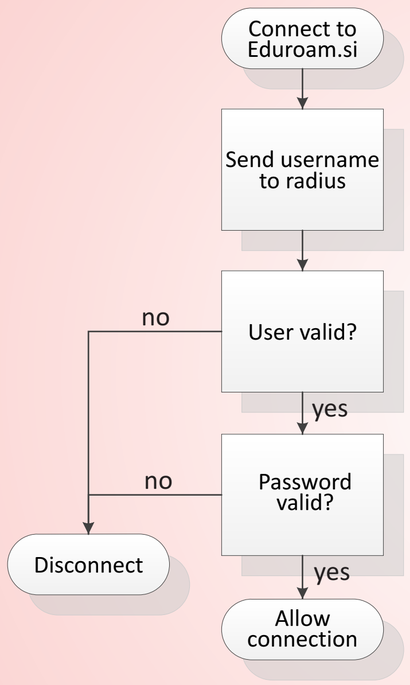
Marko Dolničar, University of Ljubljana *dolnicar.marko@gmail.com*

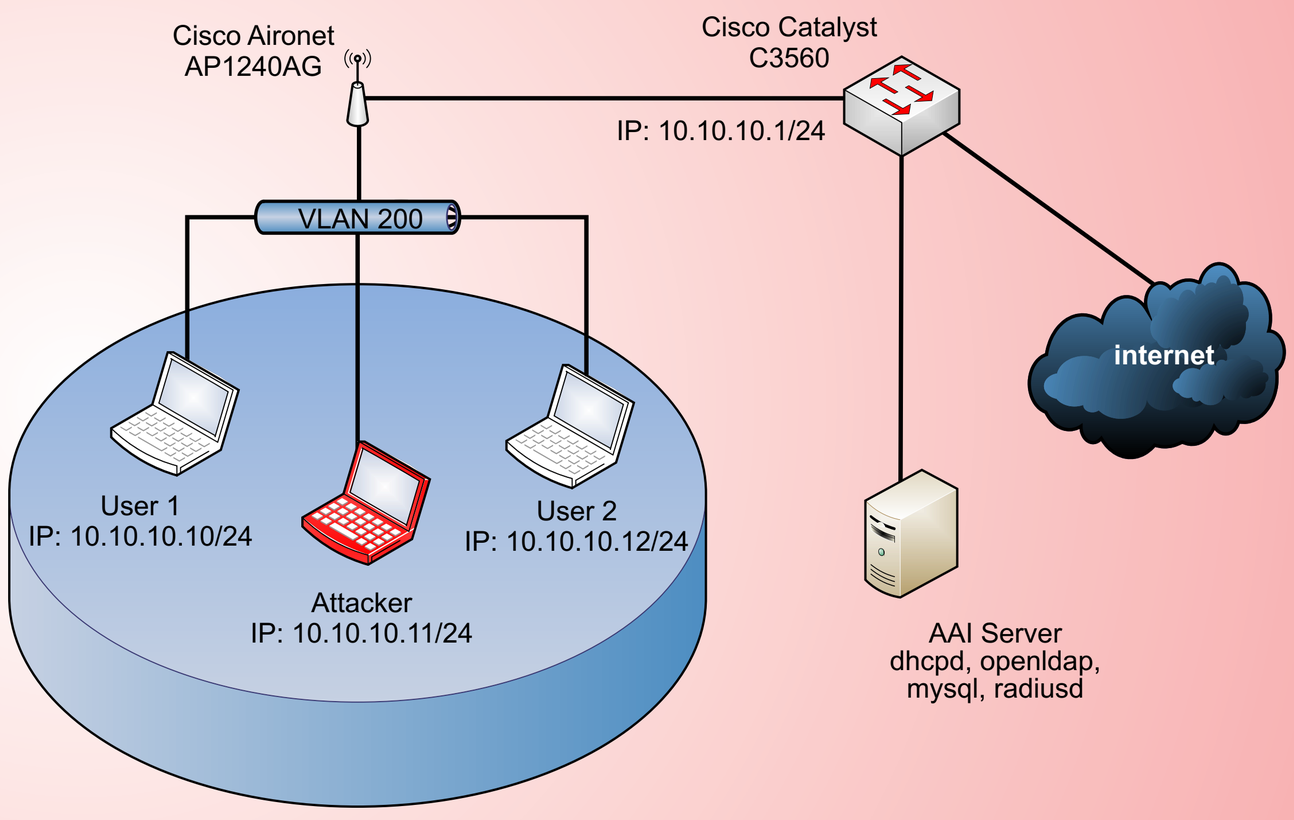
About

- Layer 2 attacks are still a threat
- Autonomous access points have no proper mitigation techniques
- Sometimes even worse - no logging

Research

- *bridge-group port-protected* command - blocks ALL communication between clients
- PVLANs - not supported on autonomous access points





Previous work

In most Eduroam.si networks all clients are on the same Layer 2 segment. This can lead to various:

- IPv4 attacks [1], e.g. ARP poisoning
- IPv6 attacks [2], e.g. IPv6 rouge RA

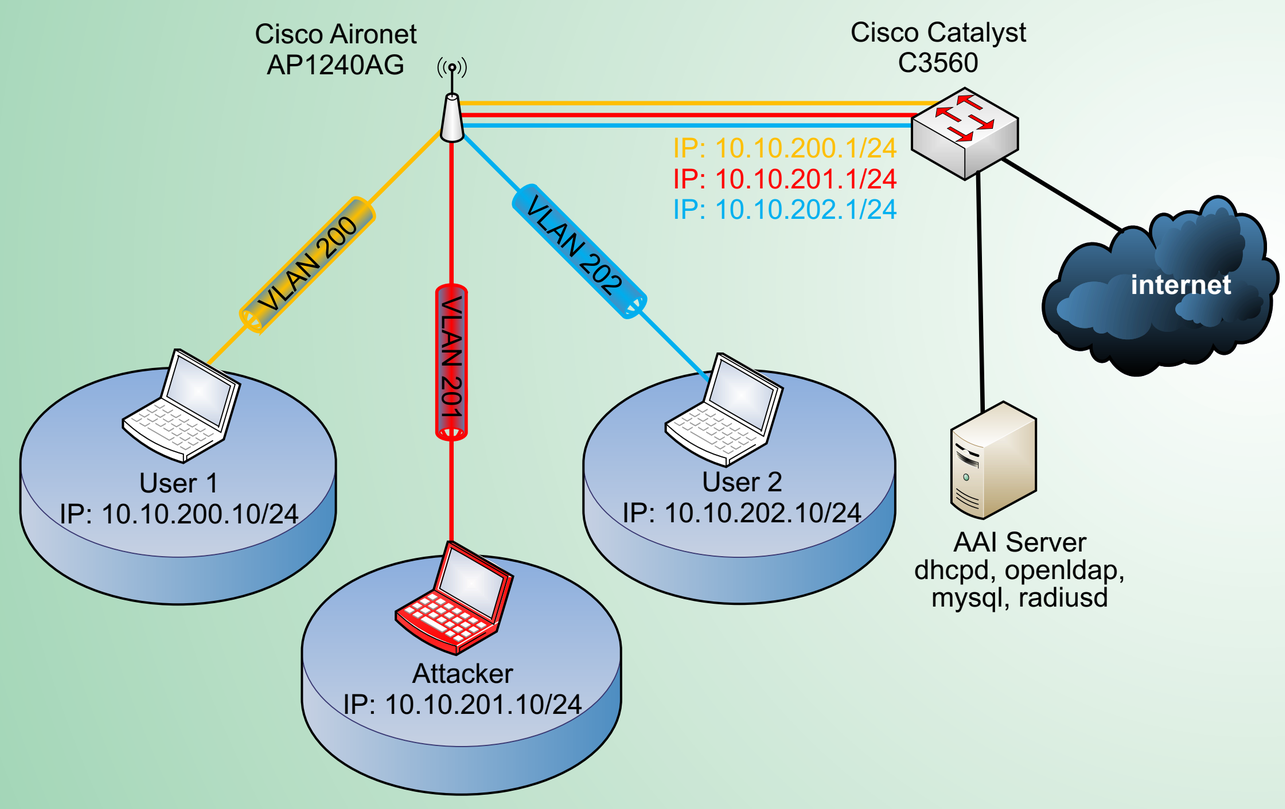
More attacks on posters:
[1] https://tnc2011.terena.org/core/poster/24
[2] https://tnc2012.terena.org/core/poster/20

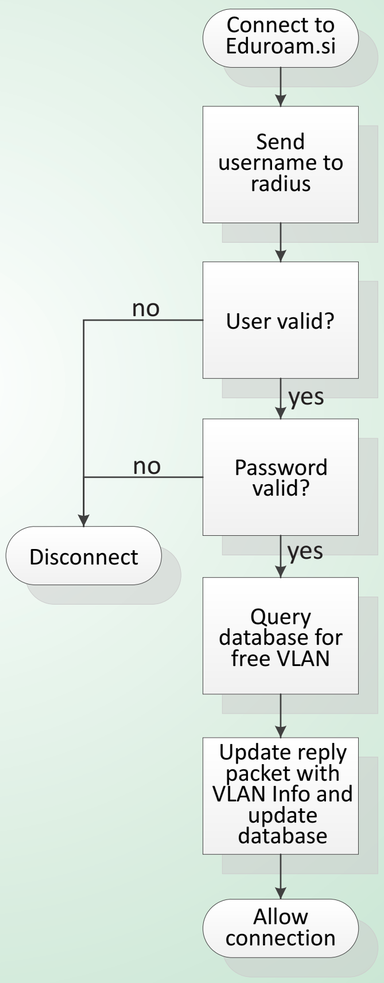
Solution

- VLAN segmentation of network: each user in a separate VLAN
- Mitigates L2 attacks

Implementation

- FreeRadius calls a script when a user connects, then updates the reply packet with VLAN attributes given from that script
- DHCP server updated with as many subnets as there are VLANs
- DHCP forwarding configured on Cisco switch to enable DHCP request/reply





Limitations

- 4 IP addresses per client (user, router, network, broadcast)
- NAT has to be used
- Maximum number of users limited to number of simultaneous VLANs supported by the switch

Future work

- This proof of concept solution stores a list of free VLANs in a text file. We would like to keep this information in a proper database
- 1:1 NAT would keep public connectivity and not waste additional public IPs - a concept that remains to be tested
- On-the-fly configuration of VLANs (as a user connects) - this would simplify base hardware configuration

Acknowledgements

We would like to thank Andrej Krevl from the Computer Communications Laboratory at the University of Ljubljana for his much appreciated mentorship and precious time he has devoted helping us.

We would also like to thank Eric Vyncke from Cisco Systems who has given the idea of VLAN separation at the TNC2012.