Security paradigms

❑ Perimeter security

- Encase the LAN with firewall / IDS / IPS to prevent any nasty stuff from getting in.
- Referred to as "M&M security"
- Hard outer shell, soft middle.

❑ Doesn't work because:

- If malware gets past perimeter, all computers become compromised.
- phishing attacks, social engineering, insiders, XSS, VPNs
- managers who are “too important” to follow procedure/policy.

Security paradigms

❑ Security policy

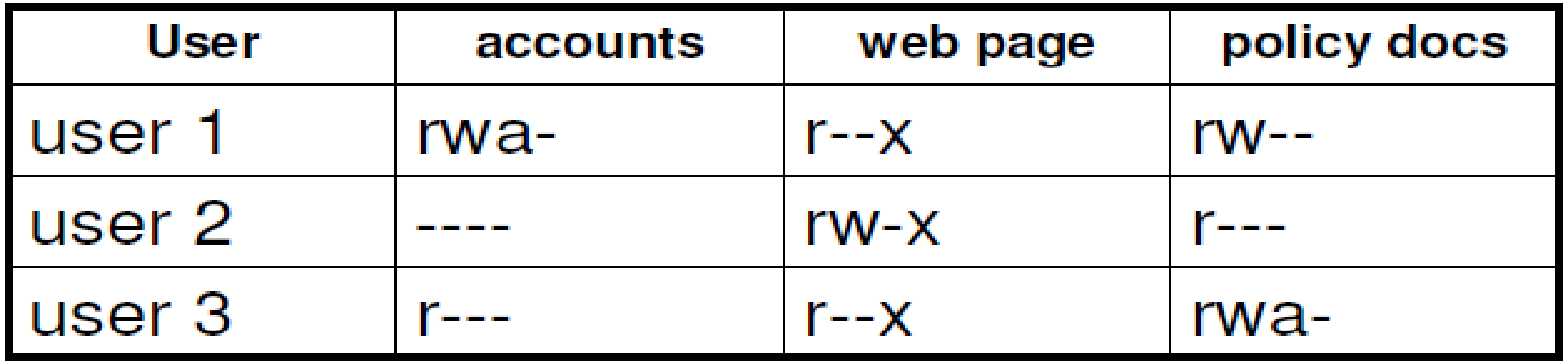
- Accidental damage or vulnerabilities may be introduced by insiders, management, visitors.
- To reduce the chances of your network users compromising the network, tell them what they are allowed to do!

- https://www.swinburne.edu.au/about/leadership-governance/policies-regulations/procedures-guidelines/acceptable-use-guidelines/

Security paradigms

❑ **Access control / User Rights Management (ACLs)**

- Both Windows and Linux support this complicated method of enforcing security.
- Individual files / directories are tagged to allow/disallow file execution, reading, writing for different user groups.
- Users are groups according to their roles / normal activities and privileges.



User	accounts	web page	policy docs
user 1	rwa-	r--x	rw--
user 2	----	rw-x	r---
user 3	r---	r--x	rwa-

Security paradigms

❑ Reactive security / Black listing

- default allow
  - Used for default installations of Windows (including Vista) and Linux assume there is only one user who is the system administrator.
  - All activities (and types of network traffic) are allowed.
  - Rules are added / ports are closed when a problem / incursion occurs.
  - Black-listing of known threats

❑ Doesn't work because:

- 0-day attacks are not known; not on black list.

Security paradigms

❑ Proactive security / White listing

default deny

- All unknown activities / ports / software are blocked until an administrator allows them.
- Allowed activities / ports / software are white-listed

❑ Hard to implement:

- push-back from users, managers, CEO.
- Requires open-minded, responsive and agile ISOs

Security paradigms

- **In Practice…**
  - Some blacklisted things
  - Some whitelisted things
  - Unknown threats slip through undetected.
  - Different policies for different resources (segmentation)
  - High-value targets are default deny, ACL;
  - Low value targets are default allow, daily re-image of SOE to minimise threat from 0-day attacks.
    - Persistent malware can defeat this

  - Need Defence in Depth because no single control is effective.

Security paradigms

- **Defence in Depth – can be based on ISO/OSI layers**

  1. Sanitise input data, filter output data
  2. ACLs, restricted rights to prevent unauthorised insiders / intruders.
  3. AV / AntiMalware on all boxes
  4. IP, network firewall, subnet firewalls, software firewalls on each PC.
  5. Physical security + screening of employees