

Computer Systems and Networks

ECPE 170 – University of the Pacific



MIPS Assembly (Random Numbers)

Random Number Generator



Random Number Generator

- MIPS syscalls do not provide a random number generator 😞
- Need to create a simple one for Lab 11
 - *Low quality - Not suitable for cryptography!*

```
m_w = <choose-initializer>; /* must not be zero */
m_z = <choose-initializer>; /* must not be zero */
uint32_t get_random()
{
    m_z = 36969 * (m_z & 65535) + (m_z >> 16);
    m_w = 18000 * (m_w & 65535) + (m_w >> 16);
    return (m_z << 16) + m_w; /* 32-bit result */
}
```

In-Class Discussion of MIPS Implementation