Minutes from I.T. Council meeting 10/16/20/17
Travis Conference Room, Bizzell Memorial Library

Attendees

Patrick Livingood, Co-Chair – Anthropology
Ron Fellhauer – IT
Burr Millsap – Administration & Finance
Aaron Biggs – Provost Office
Eddie Huebsch – IT
Chris Cook – CAPS
Andrew Fagg – Computer Science
Carol Silva – Political Science
J. Quyan Wickham - VPR
Al Schwarzkopf – Price College of Business
Elizabeth Pober – Architecture
Mark Morvant - Ctr Teaching Excellence

Meeting called to order by Patrick Livingood at 10:30

• Minutes approved
• Ron Fellhauer, Exec. Director - Security & Risk Presented this meeting
• Future of multi-factor authentication
  ◦ Duo is the product used at OU
  ◦ Security code for MFA can be sent via app, SMS, call
  ◦ Can also use hardware tokens (eg YubiKey)
    ▪ Synchronized device to provide token number
  ◦ In use today for admin access to security Tools, Support Tool 2, OU Create
    ▪ IT doing pilot with Office 365 through end of year
  ◦ Can set up frequency of challenge based on Active Directory groups
  ◦ Mobile device access not required. Can use landline phone or Duo website.
    ▪ What happens when you travel outside the country with no cell phone?
    ▪ Issue hardware token key?
  ◦ Required for accessing certain types of data
  ◦ Pre-register devices anticipated through https://accounts.ou.edu
• Internet of Things (IoT)
  ◦ 15 billion devices in 2015
  ◦ 30 billion devices by 2020
  ◦ 83 million wearable devices by 2020
  ◦ Technical/security challenges
    ▪ Authentication - who is interacting with the devices?
    ▪ Network registration of devices
    ▪ Device vulnerabilities - OS, applications, firmware: Security is secondary to
      adoption/time to market
  ◦ Sensitive/indicated data
    ▪ Critical infrastructure sensors
    ▪ Healthcare devices
    ▪ Cameras
    ▪ Wearables (emerging legal precedents)
    ▪ Vehicles
    ▪ Encryption?
  ◦ Event logging standards - there are none
Many different protocols
  ▪ IP, WiFi, Bluetooth, Z-wave...
  ▪ Data access & storage
  ▪ Authentication protocols
Physical security of devices
DDoS Capability
Best Practices
  ▪ Only connect it if is necessary
  ▪ Isolate IoT devices on a separate network / VLAN
  ▪ Assign device passwords if supported
  ▪ Patch devices - OS, apps, firmware
  ▪ Turn off Universal Plug-n-Play (UPnP)
  ▪ Do your homework on services providers