FALMOUTH UNIVERSITY

Lecture 05: A primer on network security

COMP260: Game Architecture
BSc Computing for Games

- Today’s lecture:
  - Definition of terms
  - Internet-enabled vs. Internet-centric organisations
  - Passwords

- Definition of terms

- Definition of terms
  - Key terms:
    - Vulnerability
    - Threat
    - Attack

- Definition of terms
  - Key terms:
    - Vulnerability
      - A component of a network and/or process that leaves a system open to exploitation
        - Physical issues
        - Protocol issues
        - Staff issues
        - Process issues
        - Customer issues
    - Threat
    - Attack

- Definition of terms
  - Key terms:
    - Vulnerability
      - A component of a network and/or process that leaves a system open to exploitation
        - » Physical issues
          - Location of computers, routers, cables, access points and so on
          - Physical assets can be compromised / taken / lost
            - Common to see portable devices (laptops / usb devices) ‘lost’, left behind or stolen
              - https://www.theguardian.com/politics/2008/jun/12/defence.terrorism
            - China infiltrating US firms through motherboard hacks
              - https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies
            - Data has significant value!
        - » Protocol issues
        - » Staff issues
        - » Process issues
        - » Customer issues
    - Threat
    - Attack

- Definition of terms
  - Key terms:
    - Vulnerability
      - A component of a network and/or process that leaves a system open to exploitation
        - » Physical issues
        - » Protocol issues
          - Protocols are open formats (as providers need to be able to see what they are to implement them)
          - Protocol data can be captured / copied and decoded
        - » Staff issues
        - » Process issues
        - » Customer issues
    - Threat
    - Attack

- Definition of terms
  - Key terms:
    - Vulnerability
      - A component of a network and/or process that leaves a system open to exploitation
        - » Physical issues
        - » Protocol issues
        - » Staff issues
          - Staff may use weak passwords, leave passwords in plain sight
          - Staff may be hoodwinked into revealing passwords / sensitive data
          - Staff may be coerced into revealing passwords / sensitive data
          - Disgruntled staff may reveal passwords / sensitive data for malevolent ends
        - » Process issues
        - » Customer issues
    - Threat
    - Attack

- Definition of terms
  - Key terms:
    - Vulnerability
      - A component of a network and/or process that leaves a system open to exploitation
        - » Physical issues
        - » Protocol issues
        - » Staff issues
        - » Process issues
          - Organisations may have approaches that leave them vulnerable:
            - Weak passwords as company policy
            - Poor protocol / networking approaches (HTTP vs. HTTPS, unencrypted packet data)
            - Poor data management policies (unencrypted customer data & company data)
            - Poor data disposal policies (not wiping drives on PCs, usb etc)
            - Data centre security issues
        - » Customer issues
    - Threat
    - Attack

- Definition of terms
  - Key terms:
    - Vulnerability
      - A component of a network and/or process that leaves a system open to exploitation
        - » Physical issues
        - » Protocol issues
        - » Staff issues
        - » Process issues
          - Organisations may have approaches that leave them vulnerable:
            - Weak passwords as company policy
            - Poor protocol / networking approaches (HTTP vs. HTTPS, unencrypted packet data)
            - Poor data management policies (unencrypted customer data & company data)
            - Poor data disposal policies (not wiping drives on PCs, usb etc)
            - Data centre security issues
        - » Customer issues
          - Weak passwords / shared passwords
          - Using shared machines
          - Poor wifi choices (man in the middle ‘coffee shop’)
          - Overly trusting attitude / greed (phising / boiler rooms)
    - Threat
    - Attack

- Definition of terms
  - Key terms:
    - Vulnerability
    - Threat
      - The potential for a violation of security
        - » Natural disasters
        - » Insiders or malicious and disgruntled employees
        - » Hackers
        - » Non-malicious employees
        - » Users
    - Attack

- Definition of terms
  - Key terms:
    - Vulnerability
    - Threat
    - Attack
      - An attempted violation
      - Attack = vulnerability + method + threat + motive

- Definition of terms
  - Key terms:
    - Vulnerability
    - Threat
    - Attack
      - An attempted violation
      - Attack = vulnerability + method + threat + motive
      - Motives:
        - » LoLs / Demonstrate skill
        - » need to find / share information
        - » Blackmail / financial
        - » Acquire resources
          - Physical cpu / storage / networking
          - Users / user data

- Definition of terms
  - Types of attack
    - Passive
    - Active

- Definition of terms
  - Types of attack
    - Passive
      - Traffic analysis
        - Where are packets going to?
      - Reading content
        - What is in packets?
    - Active

- Definition of terms
  - Types of attack
    - Passive
    - Active
      - Credential mis-use
        - » Stolen account details
        - » Acquired account details
        - » ‘Cracked’ account details
      - Packet fabrication
        - » Message replay
        - » Message modification
        - » Message spamming (DDoS attacks)

- Definition of terms
  - Escalation of security breaches
    - LOLs
    - Solo / team hackers demonstrate their ‘value’
    - Digital / political hacktivism
    - Financial gain
    - Blackmail
    - Building botnets

- Definition of terms
  - Escalation of security breaches
    - LOLs
      - Generally low-impact issues where accounts will be hacked for amusement, rather than serious consideration
        - Social media spoof posts
        - Comedy emails
        - etc
    - Solo / team hackers demonstrate their ‘value’
    - Digital / political hacktivism
    - Financial gain
    - Blackmail
    - Building botnets

- Definition of terms
  - Escalation of security breaches
    - LOLs
    - Solo / team hackers demonstrate their ‘value’
      - Hackers break in to (typically) US government servers to
        - » illustrate weaknesses in security (white hatters)
        - » Look for UFO evidence / whistle blowing
      - Generally get extradited to US to face long charges
        - » Laurie Love http://www.bbc.co.uk/news/uk-england-suffolk-42166200
        - » Gary McKinnon https://en.wikipedia.org/wiki/Gary_McKinnon
        - » Marcus Hutchins https://krebsonsecurity.com/2017/09/who-is-marcus-hutchins/
    - Digital / political hacktivism
    - Financial gain
    - Blackmail
    - Building botnets

- Definition of terms
  - Escalation of security breaches
    - LOLs
    - Solo / team hackers demonstrate their ‘value’
    - Digital / political hacktivism
      - Defined as ‘subversive use of computers and networks to promote a political agenda or social change
        - » https://techcrunch.com/2017/02/22/the-dramatic-rise-in-hacktivism/
        - » http://www.computerweekly.com/opinion/Hacktivism-Good-or-Evil
      - Can be government organised
        - » http://fortune.com/2017/12/11/russian-hacking-election-confession/
        - » https://www.theguardian.com/technology/2017/oct/23/kaspersky-lab-security-firm-win-trust-russian-spying-scandal-antivirus
    - Financial gain
    - Blackmail
    - Building botnets

- Definition of terms
  - Escalation of security breaches
    - LOLs
    - Solo / team hackers demonstrate their ‘value’
    - Digital / political hacktivism
      - This is spying / activism in the 21st century
        - Evidence of politically motivated DDoS attacks to bring down services
        - Hacking Isis Twitter accounts
        - Defacing websites
      - Also commercial
        - https://www.networkworld.com/article/2998251/malware-cybercrime/sony-bmg-rootkit-scandal-10-years-later.html
    - Financial gain
    - Building botnets

- Definition of terms
  - – Escalation of security breaches
    - LOLs
    - Solo / team hackers demonstrate their ‘value’
    - Digital / political hacktivism
      - – Use of Facebook data to target Brexit / US Election voting
        - » https://www.thedrum.com/news/2019/01/15/pro-brexit-ads-throw-spotlight-facebook-s-political-ad-transparency-pledge
        - » https://www.theguardian.com/uk-news/2018/nov/06/arron-banks-firm-and-leave-eu-face-135k-fine-over-data-misuse
        - » https://www.theguardian.com/politics/2018/nov/02/arron-banks-inquiry-why-is-8m-leaveeu-funding-under-review
        - » https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory
    - Financial gain
    - Building botnets

- Definition of terms
  - Escalation of security breaches
    - LOLs
    - Solo / team hackers demonstrate their ‘value’
    - Digital / political hacktivism
    - Financial gain
      - Strong driver for any illegal activities -> £££
      - Fraudulent transactions / Identity theft
        - Phishing: http://www.phishing.org/common-phishing-scams
    - Building botnets

- Definition of terms
  - Escalation of security breaches
    - LOLs
    - Solo / team hackers demonstrate their ‘value’
    - Digital / political hacktivism
    - Financial gain
      - Ransomware
        - » Encrypting user data and charging a fee to decrypt
        - » https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/10-significant-ransomware-attacks-2017/
    - Blackmail
    - Building botnets

- Definition of terms
  - – Escalation of security breaches
    - LOLs
    - Solo / team hackers demonstrate their ‘value’
    - Digital / political hacktivism
    - Financial gain
      - – Selling sensitive data
        - » Typically email addresses / credit card details taken from organisations:
        - » https://www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached
        - » https://siliconangle.com/blog/2017/12/31/forever-21-confirms-credit-card-details-stolen-hack-sales-network/
    - Blackmail
    - Building botnets

- Definition of terms
  - Escalation of security breaches
    - LOLs
    - Solo / team hackers demonstrate their ‘value’
    - Digital / political hacktivism
    - Financial gain
    - Blackmail
      - Acquiring ‘compromising’ information
        - » Webcam blackmail:
          - https://www.getsafeonline.org/social-networking/webcam-blackmail/
        - » Organisational blackmail:
          - https://www.forbes.com/sites/davelewis/2014/11/24/sony-pictures-hacked-and-blackmailed/#58e58f0d42b2
    - Building botnets

- Definition of terms
  - Escalation of security breaches
    - LOLs
    - Solo / team hackers demonstrate their ‘value’
    - Digital / political hacktivism
    - Financial gain
    - Blackmail
    - Building botnets
      - Intrinsic value of computer cpu, gpu, memory & network resources
      - Compromising PCs with software to
        - co-ordinate DDoS attacks
        - bitcoin mining ;)
        - Torrent hosts
        - Email farms

- Internet-enabled vs. Internet-centric organisations

- Internet-enabled vs. Internet-centric organisations
    - We live in an internet protocol age
        - Not all individuals and organisations have the same need or use of the internet:
        - Internet-enabled organisations
            - Organisations that use the internet for non-critical business activities
        - Internet-centric organisations
            - Organisations whose business is predicated by the internet

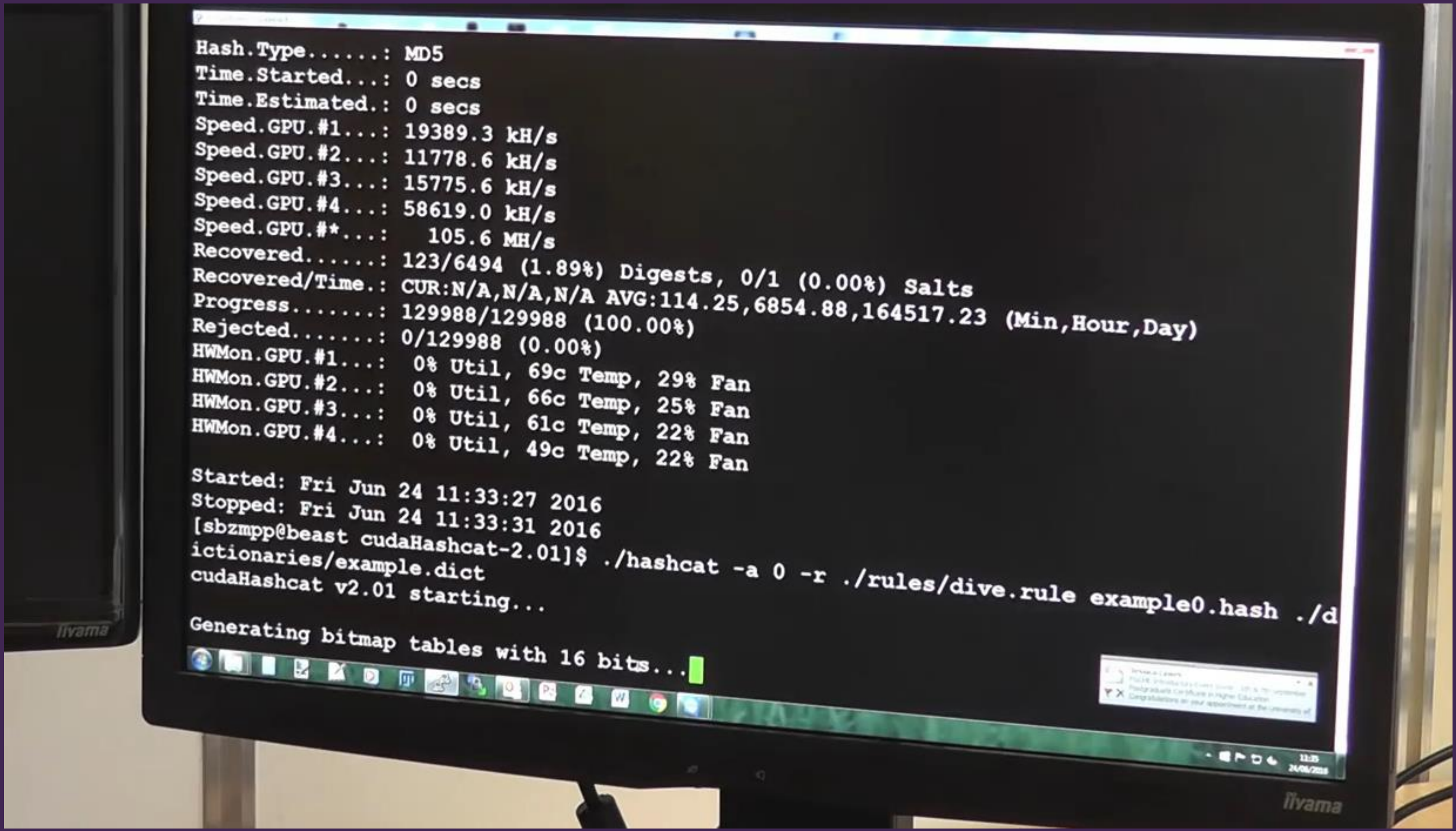
- Internet-enabled vs. Internet-centric organisations
  - We live in an internet protocol age
    - Not all individuals and organisations have the same need or use of the internet:
    - Internet-enabled organisations
      - Organisations that use the internet for non-critical business activities
        - » Banks with online banking
        - » Bricks and mortar shops with online shopping channels
        - » Offline companies with a web marketing presence (website, social media etc)
        - » Traditional products with IP components (IoT enabled toaster)

- Internet-enabled vs. Internet-centric organisations
  - We live in an internet protocol age
    - Not all individuals and organisations have the same need or use of the internet:
    - Internet-enabled organisations
      - Risk for these companies is that network security / IP understanding isn’t necessarily core to their business culture
      - Hackers will target these firms
        - » For the LoLs
        - » To prove they can
        - » For hacktivism
        - » For profit
        - » For their computing resources

- Internet-enabled vs. Internet-centric organisations
  - We live in an internet protocol age
    - Not all individuals and organisations have the same need or use of the internet:
    - Internet-centric organisations
      - Organisations whose business is predicated by the internet
        - Social media companies (Twitter, FB, blogging)
        - Purely on-line stores and services (Amazon, ebay, Steam)
        - GaaS (WoW, Clash of Clans etc)
        - Technology service providers (github, trello, teamviewer, google, yahoo etc)

- Internet-enabled vs. Internet-centric organisations
  - We live in an internet protocol age
    - Not all individuals and organisations have the same need or use of the internet:
    - Internet-centric organisations
      - Risk for these organisations is that their entire business is (generally) predicated around being secure
        - » Being insecure suggests an existential issue
      - Hackers will target these firms
        - » For the LoLs
        - » To prove they can
        - » For hacktivism
        - » For profit
        - » For their computing resources

- Passwords



```
Hash.Type.......: MD5
Time.Started...: 0 secs
Time.Estimated.: 0 secs
Speed.GPU.#1...: 19389.3 kH/s
Speed.GPU.#2...: 11778.6 kH/s
Speed.GPU.#3...: 15775.6 kH/s
Speed.GPU.#4...: 58619.0 kH/s
Speed.GPU.#*...:   105.6 MH/s
Recovered......: 123/6494 (1.89%) Digests, 0/1 (0.00%) Salts
Recovered/Time.: CUR:N/A,N/A,N/A AVG:114.25,6854.88,164517.23 (Min,Hour,Day)
Progress.......: 129988/129988 (100.00%)
Rejected.......: 0/129988 (0.00%)
HWMon.GPU.#1...:  0% Util, 69c Temp, 29% Fan
HWMon.GPU.#2...:  0% Util, 66c Temp, 25% Fan
HWMon.GPU.#3...:  0% Util, 61c Temp, 22% Fan
HWMon.GPU.#4...:  0% Util, 49c Temp, 22% Fan

Started: Fri Jun 24 11:33:27 2016
Stopped: Fri Jun 24 11:33:31 2016
[sbzmpp@beast cudaHashcat-2.01]$ ./hashcat -a 0 -r ./rules/dive.rule example0.hash ./d
ictionaries/example.dict
cudaHashcat v2.01 starting...

Generating bitmap tables with 16 bits...
```

  - A short video on why your passwords are terrible

- Conclusions

- Conclusions
  - ‘Hackers’ want to get into computer systems as the system have inherent value
    - Financial value
    - Value of data
    - Value of visibility / eyeballs
    - Value of accomplishment

- Conclusions
  - Generally with security, human factors are the weakest and easiest to exploit
    - Employees and users have their own needs that are not always aligned to good security
      - Ease of use vs. strength of security
        - » Easy to remember passwords vs. Strong passwords
        - » Storing vs. Remembering
        - » Sharing vs. Security
        - » 2FA is a pain if you are in a poor mobile area
        - » In transaction checks ‘slow’ people down
      - People assume the best of intentions
        - » Ideal for phishers

Questions?