# Lecture 1: Intro

## Course Intro

Assessments:

* Coursework 20%
* Labs 10%
* Quizzes 10%
* Exam 60%

Schedule

* Every Monday
* Lectures 12:00 – 14:00 online
* Labs 14:00 – 16:00

Expectations:

* Personal research on most problems
* Lecture material only is not enough; participation is needed
* Discuss with colleagues
* Come to own conclusions with justifications

## Content Intro

Data to protect:

* Personal
* Confidential docs
* Operational
* Apps – API/Services
* Transactions
* Social Media

Defence

* Defence in depth/Layered approach:
  + Chart

    Description automatically generated
  + Perimeter Scanner
    - Vulnerability scanning [TO BE CONTINUED]
    - Used in big organisations
  + IDS/IPS
    - Intrusion Detection System
      * Monitors traffic and alerts
    - Intrusion Prevention System
      * Acts when identifies
  + Firewall
    - Barrier between trusted internal and untrusted external network
    - Packet inspection
    - Does not alert
  + Proxy
    - Intermediary for requests by clients accessing server
    - Evaluating
  + End Point/AV (Antivirus)
    - Security software installed
    - Updates located there
    - End point – behaviour antivirus, identifies patterns

Cyber Attack Techniques

* Passive
  + Information Gathering
  + Vulnerability Scan
  + Usually, first step of a more complex & long-term attack
* Active
  + Gain access
  + Disruption & damage of service (DoS)
  + Usually short-term

Cyber Attack Goals

* Data loss/Leakage
* Reputation
* Financial
* Disruption
* Loss of life

Type of attackers

* Hacktivists
* Malicious insider
* Malicious outsider
* Attack by accident
* Government
* Competitors

## Tutorial

Question 1: Difference between https: and http:

* Https uses Transport Layer Security to increase security by encryption

Q2: 4 criteria for passwords:

* No personal data (name, date of birth, favourite \_\_\_)
* Preferably not used anywhere else (who does this though (except people who use password managers)?)
* Memorable to self
* Long, but not too long (for memorability/efficiency)

Q3: Human factor as a factor in cyber security. Yes/No, why?

* Yes
* Ignorance of/Apathy to safe practices, weakness to phishing, sharing in social media,

Q4: Cyberwarfare, discuss definition and importance with examples

* Different definitions:
  + In common: cyber attack from one nation state to another
  + To do physical damage, or
  + To enable all-out war (or comparable harm), or
  + WannaCry?

Q5: Cyber-attack, discuss (type, impact, techniques used). How to avoid?

* Sony Pictures Hack of 2014
* Type: Passive, then active
* Impact: Data loss/leakage
* Techniques:
  + malware
    - Server Message Block (SMB) Worm Tool (Brambul)
    - Worm – standalone malware that spreads to other computers
    - Components:
      * listening implant
      * backdoor
      * proxy tool
      * destructive hard drive tool
      * destructive target cleaning tool
* How to avoid: don’t know, increase security

Q6: Public free Wi-Fi. Safe? How to increase security while using it

* Not safe at all
* Use VPN? Proxies? More secure browsers, like Tor?

Q7: Cloud services. Pros/cons (in CyberSec)

* Pros:
  + If there are security measures in place, they might be better than local ones/no time wasted in creating same measures
* Cons:
  + Dependence on third party, they might be more vulnerable
  + No knowledge of their intentions/capabilities
    - Trust
  + Less freedom in how to secure data
  + Increase in potential attack places

# Week 2: Basic Networking

TTL – time to live

## Tutorial

Q1:

|  |  |  |
| --- | --- | --- |
| Port no. | Protocol | Description |
| 23 |  |  |
| 53 |  |  |
| 43 |  |  |
| 20 |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Q3:

* A – IP address
* AAAA – IPv6 address
* SSHFP – SSH public key fingerprint

Q4: 2 – IPv4 and IPv6 (longer)

Q5:

* MAC address – 00:0a:95:9d:68:16
* DNS – AAAA
* IPv4 address – 192.168.43.58
* IPv6 address – 2001:db8:85a3:0:0:8a2e:370:7334
* Domain address – [www.bbc.co.uk](http://www.bbc.co.uk)

Q4: Range of local IPv4:

* Class A: 10.0.0.0 — 10.255.255.255
* Class B: 172.16.0.0 — 172.31.255.255
* Class C: 192.168.0.0 — 192.168.255.255

Q5:

1. Someone accessing Glasgow Uni website
2. Protocols:
   1. DNS
   2. TLS
   3. TCP
   4. HTTP
3. Details:
   1. Source:
      1. IP: 10.0.2.15
      2. Port: 39769
   2. Destination:
      1. IP: 192.168.1.254
      2. Port: 53
4. Notable:

# Week 3: Web Attacks Intro (Phishing, DDoS,

News:

* [www.telegraph.co.uk](http://www.telegraph.co.uk)
* [www.bbc.co.uk](http://www.bbc.co.uk)
* [www.ncsc.gov.uk](http://www.ncsc.gov.uk)
* [www.thehackernews.com](http://www.thehackernews.com)

Statistics:

* [www.csis.org](http://www.csis.org)

Tools (for detecting malicious URLs, files)

* URLS:
  + <https://urlscan.io/>
  + <https://checkphish.ai/> (also IP lookup)
* Files (check phishing email attachments):
  + <https://app.any.run/>
* <https://www.hybrid-analysis.com>

## Tutorial

Q2:

1. Pulsing zombie – degradation-of-service attack, sending steady stream of attacks over a long period of time
2. Shoulder surfing – theft of data by looking over user’s shoulder
3. Sandbox – isolated environment on a network that mimics end-user operating environments, catches security risks (no risk of infecting actual device/network)
4. Dumpster diving – searching through trash for sensitive data
5. Walled garden – environment that controls/restricts the user’s access to network-based content and services

Q3: Spyware – malicious software used to gather and publish/access info. Gathers info by logging computer activity, e.g., keyloggers. Ex: Loverspy, used for stalking.

Q4: Hardest procedures for attackers: not getting caught (traced),

# Week 4: Web App Attacks (OWASP Top 10)

# Week 6: Cryptography

# Week 9: Guest Lectures

## Guest Lecture 1: Bitcoin & Blockchain

by Nguyen ???

In general:

* Distributed, decentralised digital currency system
* Effectively, a bank run by an ad-hoc (peer-to-peer) network
  + Digital checks
  + Distributed transaction log
* Released by Satoshi Nakamoto in 2008

Timeline:

* 2040 BC
  + Mesopotamia
  + Balance sheet
* 1848
  + BNP PARBAS

Differences with traditional

* Centralised ledger
  + Identity: sort-code/account number
  + Authentication: physical bank card, internet/mobile banking account
  + Transactions: verified and recorded (onto the ledger) by central bank
* Distributed ledger:
  + Identity: public-key, e.g., Bitcoin address = hash of hash of public-key
  + Authentication: digital signature
  + Transactions: verified and recorded (onto distributed ledger, e.g., Bitcoin blockchain, by participants in the network

Cryptography

* Public-key encryption
  + Key pair: public and private key
    - Bitcoin: Elliptic Curve Secp256k1
* Digital Signatures
  + First, create message digest using a cryptographic hash
  + Then, encrypt message digest with your private key
  + In Bitcoin, SHA256

Bitcoin Protocol

* Bitcoin Addresses
  + Identity: each user owns a private/public key pair
  + BTC address generated from user’s public key
    - Unique id
    - Hash of hash of public key
  + Total Balance < 21M BTC
  + Satoshi == 10-8­ Bitcoin
* Bitcoin Ledger: Blockchain
  + Distributed ledger – chain of blocks
  + Each block contains Header and Transactions
  + Nodes in Bitcoin network are expected to store exactly the same …?
  + Block
    - Header
      * Serialised in the 80 byte format
      * Version
      * Prev. Block header hash
        + Ensures no previous blocks can be changed without changing this one
      * Merkle Root hash
      * Time
      * Nonce:
* Transactions
  + Data Types: Merkle Tree
    - Root hash of Merkle tree is written in the header
    - If any transaction is modified, then the root hash is changed
    - => change of hash of Block header
  + Data Type: “Input”, “Output”, and other params
  + Input of transaction is output of another transaction
    - ex: Alice needs to prove she has 1BTC that she wants to send by showing her receiving that 1BTC from another transaction
  + Outputs: define conditions using a scripting system
    - Conditions must be satisfied in order to spend the output in the next transactions
* Scripting System
  + Stack-based programming language
  + if true, transaction is valid
  + Many opcodes defined
* Consensus Mechanism: Proof-of-work
  + Core of BTC is distributed ledger blockchain, therefore:
    - Information added to the ledger must be accurate and honest
    - Entire network agrees with ledger’s content
  + Mechanism for all nodes in BTC network to cooperate and reach a common opinion (consensus)
  + Nonce?
    - Number only used once
    - Some nodes in the Bitcoin network try to find Nonce N s.t.:
      * Hash(Hash(B3)|txs|N) < target
        + target – controls difficulty
        + Best known approach: Brute Force
      * this process is known as mining, and the nodes are miners
  + When miner finds Nonce, correctly forms a new block
  + Proof-of-work: Update Rule and Forks
    - What happens if some miners successfully calculate Nonce and broadcast their own block to the network
      * Network partition
      * Fork
        + Soft: temporary
        + Hard – permanent
    - Update Rule
      * Longest chain wins
      * Eventually, all the nodes will have the same blockchain (longest one)
* Security
  + Authentication: Public Key Crypto (Digital Signatures)
  + Availability: Broadcast messages to the P2P network
  + Why proof-of-work?
    - Integrity
      * To prevent from transaction alteration/reverse and double-spend
      * Intuitively, to change/reverse Tx, a malicious miner needs to recompute nonce for several blocks while racing with other host miners for new block
  + Double Spend attack
    - Attacker executes a transaction that attacks carried out before payment
    - Secretly mining using the block that includes this last transaction
    - Wait for the transaction sending the money to victim V to receive enough confirming blocks
      * V hands over goods, sure that the money is finally appropriated to them
    - Continue to mine the secret alternative branch until it becomes more than public, after which it is broadcast to the network
      * Since the new branch is longer than all others, it will be considered valid, and BTC transfers to V will be replaces by sending coins to the attacker
    - Practically impossible in Bitcoin
      * Need >50% computational power of the whole Bitcoin network (51% attack)
      * Mining pools
        + Probability of finding a block alone is very small
        + Unite in Mining pools
        + Payout is done proportional to the work
        + What if the mining pools collude and carry out double-spend attack?
  + Pseudonymity
    - Pseudo-anonymous due to BTC addresses
    - Wrong:
      * Alice’s BTC relates to each other due to the definition of transactions
      * Combined with other side-info/low-layer network info (IP addresses, etc) in the Bitcoin network
      * There is a change of figuring out the real identity of BTC owners
    - Solutions:
      * Mixer, JoinCoin, k-anonymity Privacy, n-anonymity privacy, Zero-Knowledge-Proof

## Guest Lecture 2: CyberSec in IoT Networks

by Dongzhu Liu

Internet of Things (IoT)

* System of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction
* All electronic devices that can collect, transform data over networks
* Applications
  + Smart Street Parking
  + Smart Manufacturing
  + Sleep Monitoring
  + Connected Vehicles
* Features
  + Heterogeneity
    - Data/computing/storage
  + Sensing
    - Obtain data to perform analysis
  + Enormous Scale
    - From smart home to smart city
  + Intelligence
    - Automatic response without manual intervention
  + Connectivity
    - Communicate through various protocols
  + Dynamic Nature
    - Adapt to context
* How does it work?

1. Sensors/Devices
   1. Collecting data
   2. ex: temperature reading, video feeds, not just a simple sensor (mobile phone)
2. Connectivity
   1. Sending data to cloud
   2. ex: cellular, satellite, Wi-Fi, Bluetooth, low-power WANs (LPWAN), or ethernet, depending on trade-offs between power consumption, range and bandwidth
3. Data Processing
   1. Making data useful
   2. Simple task (check temp reading) or complex (identify objects in video)
   3. Edge Computing
      1. Near to sensors/devices
      2. Fast Response
      3. Ubiquitous Computing
      4. Security
4. User Interface
   1. Delivering info to user
   2. ex: temperature alert -> action on system (manual/auto)
   * Layers
     + Application
       - Smart Factory, Healthcare, Transport
     + Transportation
       - Cellular,
     + ???

* Pros
  + Real-time data collection
  + Minimise human effort, save time
  + Increased security – provide services, ex: monitor and smart control
  + Efficient resource allocation
  + Useful for safety concerns, healthcare
* Cons:
  + Security issues, ex: network attacks
  + Privacy, ex: personal data
  + Complexity of system (design, developing, maintaining)
  + Lack of international standardisation
  + High dependency on Internet
  + Inadequate storage capacity

Security

* Weakness
  + Vulnerable as devices lack necessary built-in security controls to defend against attacks
    - Reason: constrained environment and the limited computational capacity that permit only certain functions and fail to support security controls and data protection schemes
  + Top 10:

1. Weak/guessable/hardcoded passwords
   1. Use of easily brute-forced/publicly available/unchangeable credentials, including backdoors in firmware/client software that grants unauthorised access to deployed systems
2. Insecure Network Services
3. Insecure ecosystem interfaces
   1. Insecure web/backend API/cloud/mobile interfaces in ecosystem outside of the decision that allows compromisation of device/its related components. Common issues – lack of authentication
4. Lack of secure update mechanism
   1. Vulnerabilities discovered once product is deployed. Common problems – lack of TLS/SSL communication to deliver the software updates
5. Use of insecure/outdated components
   1. Ultimately, everything gets outdated. Often vendors stop manufacturing and software up-gradation. Then, no patches come in future, places
6. Insufficient privacy protection
7. Insecure data transfer and storage
8. Lack of device management
9. Insecure default setting
10. Lack of physical hardening

Four-Layer Architecture

* Secure Device
  + Feature
    - Chip security
      * Don’t release encryption keys outside chip
    - Secure booting
    - Physical security protection
  + Principles
    - 1) Device intelligence
      * Required for complex tasks
    - 2) Edge processing
* Secure Communications
  + Feature
    - Data-centric security solutions – ensure data is safely encrypted while in transit
    - Firewalls and intrusion prevention systems – examine specific traffic flows terminating at the device, detect unwanted intrusions and prevent malicious activities on the communication layer
  + Principles
    - 3) Device-initiated connections
      * Initiate connection to cloud, not vice versa
      * Devices are not likely to be supported to same degree of protection as server
    - 4) Messaging control
      * Inherit security
* Secure Cloud
  + Feature
    - Sensitive information stored in cloud (data at rest) must be encrypted – avoid exposure to attacks
    - Verify integrity of other cloud platforms/3rd party apps
    - Digital certificates
  + Principle
    - 5) Identification, authentication, encryption
* Secure Lifecyle Management
  + Feature
    - Activity monitoring plays important role – track, log, detect suspicious activity
    - Regular security patches for devices/apps
    - Secure remote control – maintain billions of devices
  + Principle
    - 6) Remote control and updates of devices

Challenges & Opportunities

* Challenges
  + Security
    - Unsecure devices
    - Network can block unwanted traffic or detect suspicious behaviour
  + Network
    - Scalability
    - Diversity
    - Open network interface
    - Low-power communication
  + Software Development
    - Big data (volume, variety, velocity)
    - Self-configuration (SW, HW, networking configuration)
  + New and Complex Dependencies
    - Modelling human behaviours (human-in-the-loop)
* Opportunities

# Week 10: Digital Forensics