INTRO TO ETHICAL HACKING

MIS 5211.001

Week 11

Site:

https://community.mis.temple.edu/mis5211sec702fall2020/

1

Tonight's Plan

- Cloud Primer
- Wireless

2

Cloud

- First things First
- There is no cloud
  - It is just somebody else's computer
- No magic
- Nothing "Special"

3

Cloud vs Virtualization

- First question I asked many years ago was "What is the difference between virtualization and Cloud. Here's the answer I eventually got.
- Cloud is just a virtualized environment with an additional layer of management tooling.
  - This answer still seems to make sense.

MIS 5211.001 4

4

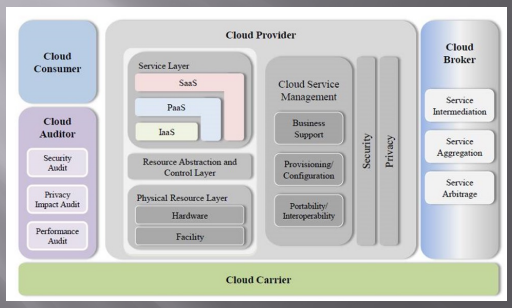
More Cloud Basics

- From NIST:
  - "Cloud computing is a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

MIS 5211.001 5

5

NISTs Picture



http://pleasediscuss.com/andimann/20110330/new-cloud-reference-architecture-from-nist/nist-cloud-ref-architecture/

MIS 5211.001 6

6

Cloud Drivers

- Elasticity
  - Virtualization
  - Scalability
- Simplicity
  - Risk Reduction
  - Cost
- Expandability
  - Mobility
  - Collaboration and Inovation

7

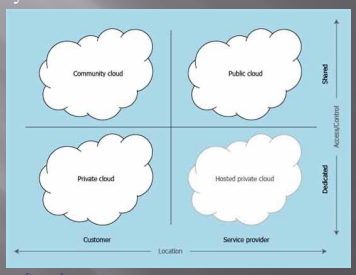
Cloud Providers

https://media.amazonwebservices.com/blog/2019/gartner_iaas_mq_2019_800px_1.jpg

8

Cloud Definitions

- Deployment Models



https://technet.microsoft.com/en-us/library/hh509051.aspx.

9

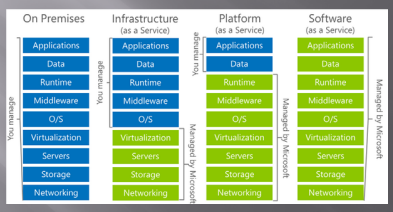
Cloud Definitions

- More on Deployment Models
  - Private – Provided for exclusive use of a single organization
  - Community – Provided for exclusive use of a specific community
  - Public – Open to use by all
  - Hybrid – Mix from above

10

Cloud Definitions

- Service Models



https://blogs.partner.microsoft.com/mpn-canada/transitioning-premises-virtual-machines-cost-effective-azure-cloud-models/

11

Cloud Definitions

- Infrastructure
  - Cloud provider hosts your server build and may host virtual network components that you are responsible for
- Platform
  - Cloud provider hosts their server and infrastructure, and you can run your applications
- Software as a Service (SaaS)
  - Provider runs everything, you just use the software
  - Think Office 365, Exchange in the cloud, etc…

12

Key Cloud Security Concept

- Cloud provider is responsible for "**Security of the Cloud**"
- Cloud user is responsible for "**Security in the Cloud**"
- Example: If you build a server in the cloud, it is your job to harden the system and ensure proper access controls

MIS 5211.001 13

13

Network Security

- Generally provided by the Cloud Host
- You will have very limited (read none) access to logging or info from the cloud providers systems
- You can sometimes install virtual appliances inside of the cloud such as firewalls, load balancers, etc.

MIS 5211.001 14

14

Cryptography

- Cloud providers will generally encrypt data at rest
  - However, it is their key(s)
  - May want to also encrypt with your key(s)
- Should also provide for encryption in transit
  - Should be evaluated during negotiations as to what is possible

MIS 5211.001 15

15

Access Control

- Need to cover
  - Provisioning and deprovisioning
  - Centralized directory services
  - Privileged user management
  - Authorization and access management
    - Especially the difference between authentication and authorization

MIS 5211.001 16

16

Data Sanitation

- Should discuss "before" signing the contract
- Options:
  - Cryptographic erasure – encrypt and throw away the key
  - Overwriting
- Note. Drive destruction is not really an option in a cloud environment as data from multiple clients may reside on the same drive and your data may be spread across many drives

MIS 5211.001 17

17

Virtualization Security

- Type I Hypervisor - Running directly on the hardware with virtual machine (VM) resources provided by the hypervisor. These are also referred to as "bare metal" hypervisors. Examples of these include VMware ESXi and Citrix XenServer.
- Type II Hypervisor - Run on a host OS to provide virtualization services. Examples of Type II are VMware Workstation and Virtual Box.

MIS 5211.001 18

18

Hackers view of Type I/II

- Type II is still an OS, likely to have a greater attack surface

19

Common Threats

- Breach
- Data Loss
- Account Hijacking
- Insecure APIs
- Malicious Insiders (Provider and User)
- Abuse of Cloud Services *
- Insufficient Due Diligence *
- Shared Technology Vulnerabilities *

20

Abuse of Cloud Services

- Think password cracking on steroids
- Brute forcing encryption

21

Insufficient Due Diligence

- Cloud development can out pace governance
  - Who's creating guests
  - Are guest machines being shutdown
  - Was there even a business case
  - How much is being done on procurement cards and click through agreements
  - Can anyone in the company even answer the questions above

MIS 5211.001 22

22

Shared Technology Vulnerabilities

- Cloud provider business case requires sharing of resources.
- Your guest machine is on the same host as your competitor (or your attacker)
- Your data is on the same wire, just logically seperated

MIS 5211.001 23

23

IaaS Concerns

- Virtual machine attacks
- Virtual network attacks
  - Switches
  - Routers
  - NICs
- Hypervisor Attacks
- Denial of Service

MIS 5211.001 24

24

IaaS Concerns

- Multitenancy
- Workload Complexity
- Network Topology
- Logical Network Segmentation
- No physical endpoints
- Single Point of Access

MIS 5211.001 25

25

PaaS

- System and Resource Isolation
- User Level Permissions
- User Access Management

MIS 5211.001 26

26

SaaS

- Data Segregation
- Data Access and Policies
- Web Application Security

MIS 5211.001 27

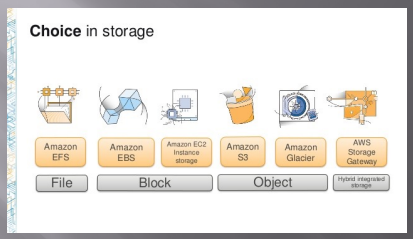
27

Data Security

- Storage
  - Volume Storage – Think hard drive for a virtual machine like Amazon EBS
  - Object Storage – Think file share like Amazon S3
  - Database – As name implies, database as a service, think Amazon Database Services on EC2 or EBS
  - Big Data – Data Analytics

28

Amazon Storage Picure



https://pt.slideshare.net/AmazonWebServices/stg201-state-of-the-union-aws-storage-services

29

Key Management

- Challenges
  - Access to Keys
  - Key Storage
  - Backup and Replication
- Considerations
  - Random Number Generation
  - No transmission in clear text
  - No storage in clear text
  - Key escrow

30

Masking, Obfuscation, and Anonymization

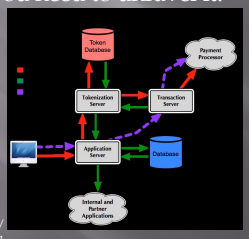
- Masking
  - Random substitution
  - Algorithmic substitution
  - Shuffle
  - Masking (Specific characters)
  - Deletion
  - Primary methods of masking data
    - Static: In static masking, a new copy of the data is created with the masked values. Static masking is typically efficient when creating clean, nonproduction environments.
    - Dynamic: Dynamic masking (sometimes referred to as on-the-fly masking) adds a layer of masking between the application and the database

MIS 5211.001 31

31

Tokenzation

- Substitute with a token value
- Token to real value table maintained internally in case you need to unravel it.



https://securosis.com/blog/tokenization-use-cases-part-1

MIS 5211.001 32

32

Global

- One cloud consideration is geographic
- Many nations have rules about where their citizens data resides
- This may restrict what can go in which cloud
- Most major cloud providers offer regional data centers to address this issue.

MIS 5211.001 33

33

Cloud Attack Vectors

- Cloud computing introduces external service providers.
- Guest escape
- Identity compromise, either technical or social
- API compromise, for example by leaking API credentials
- Attacks on the provider's infrastructure and facilities
- Attacks on the connecting infrastructure (cloud carrier)

MIS 5211.001 34

34

Identity and Access Management

- Some form of LDAP (Active Directory)
- Federated Identities
  - SAML (Security Assertion Markup Language)
  - WS-Federation
  - Open-ID
  - OAuth
- Multifactor Authentication
  - Especially for privileged accounts

MIS 5211.001 35

35

Other Technologies

- WAF – Web Application Firewall
- DAM – Database Activity Monitoring
- XML Gateways
  - DLP
  - AV
- Firewalls
- API Gateways
  - Access control
  - Rate limiting
  - Metrics
  - Security Filtering

MIS 5211.001 36

36

Application Virtualization

- Sub-category of "Sand Boxing"
- Application runs in a memory bubble (App-V) isolated from OS services and other applications

MIS 5211.001 37

37

Cloud Vulnerabilities

- Area to watch
  - Cloud Security Alliance
    - https://cloudsecurityalliance.org
  - RedLock Blog
    - https://redlock.io/blog

MIS 5211.001 38

38

OWASP Cloud - 10 Project

- OWASP Cloud-10 Candidates
  1. Insecure cloud, container or orchestration configuration
  2. Injection flaws (app layer, cloud events, cloud services)
  3. Improper authentication & authorization
  4. CI/CD pipeline & software supply chain flaws
  5. Insecure secrets storage
  6. Over-permissive or insecure network policies
  7. Using components with known vulnerabilities
  8. Improper assets management
  9. Inadequate 'compute' resource quota limits
  10. Ineffective logging & monitoring (e.g. runtime activity)
- https://owasp.org/www-project-cloud-native-application-security-top-10/

MIS 5211.001 39

39

Free Training

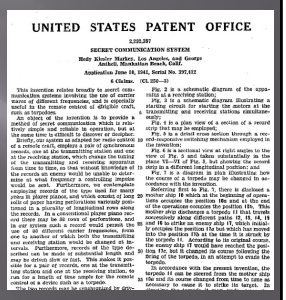
- Amazon offers a free three hour online security course
- https://aws.amazon.com/training/course-descriptions/security-fundamentals/
- Course Outline:
    - Introduction to Cloud Computing and AWS Security
    - Access Control and Management
    - AWS Security: Governance, Logging, and Encryption
    - Compliance and Risk Management

Wireless Security

- First, a small bit of trivia:
- Who invented the technology we now think of as WiFi?

The Answer

The Actress Hedy Lamar



UNITED STATES PATENT OFFICE

2,292,387

SECRET COMMUNICATION SYSTEM

Hedy Kiesler Markey, Los Angeles, and George
Antheil, Manhattan Beach, Calif.

Application June 10, 1941, Serial No. 397,412

6 Claims. (Cl. 250—2)

This invention relates broadly to secret communication systems involving the use of carrier waves of different frequencies, and is especially useful in the remote control of dirigible craft, such as torpedoes.

An object of the invention is to provide a method of secret communication which is relatively simple and reliable in operation, but at the same time is difficult to discover or decipher.

Briefly, our system as adapted for radio control of a remote craft, employs a pair of synchronous records, one at the transmitting station and one at the receiving station, which change the tuning of the transmitting and receiving apparatus from time to time, so that without knowledge of the records an enemy would be unable to determine at what frequency a controlling impulse would be sent. Furthermore, we contemplate employing records of the type used for many years in player pianos, and which consist of long rolls of paper having perforations variously positioned in a plurality of longitudinal rows along the records. In a conventional player piano record there may be 88 rows of perforations, and in our system such a record would permit the use of 88 different carrier frequencies, from one to another of which both the transmitting and receiving station would be changed at intervals. Furthermore, records of the type described can be made of substantial length and may be driven slow or fast. This makes it possible for a pair of records, one at the transmitting station and one at the receiving station, to run for a length of time ample for the remote control of a device such as a torpedo.

The two records may be synchronized by driv-

Fig. 2 is a schematic diagram of the apparatus at a receiving station;

Fig. 3 is a schematic diagram illustrating a starting circuit for starting the motors at the transmitting and receiving stations simultaneously;

Fig. 4 is a plan view of a section of a record strip that may be employed;

Fig. 5 is a detail cross section through a record-responsive switching mechanism employed in the invention;

Fig. 6 is a sectional view at right angles to the view of Fig. 5 and taken substantially in the plane VI—VI of Fig. 5, but showing the record strip in a different longitudinal position; and

Fig. 7 is a diagram in plan illustrating how the course of a torpedo may be changed in accordance with the invention.

Referring first to Fig. 7, there is disclosed a mother ship 10 which at the beginning of operations occupies the position 10a and at the end of the operations occupies the position 10b. This mother ship discharges a torpedo 11 that travels successively along different paths 12, 13, 14, 15 and 16 to strike an enemy ship 17, which initially occupies the position 17a but which has moved into the position 17b at the time it is struck by the torpedo 11. According to its original course, the enemy ship 17 would have reached the position 17c, but it changed its course following the firing of the torpedo, in an attempt to evade the torpedo.

In accordance with the present invention, the torpedo 11 can be steered from the mother ship 10a and its course changed from time to time as necessary to cause it to strike its target. In

- Source: http://www.pixmule.com/hedy-lamarr/ and https://en.wikipedia.org/wiki/Hedy_Lamarr#/media/File:Lamarr_patent.png

Security vs Mobility

- Wireless is different
  - Physical security is no longer relevant
    - Access from outside perimeter
    - Users connecting to "other" networks
  - Users and Networks are vulnerable even when not in use

MIS 5211.701 43

43

More Issues

- Attack tools are cheap
  - Hardware is close to zero
  - Software is zero
- Segregation doesn't work
  - Even with "guest" networks, they are still on your wires and can still cause you issues
- Fallacy of "We don't have any wireless"
  - No, you just don't know about the wireless you have

MIS 5211.701 44

44

Still More Issues

- Encryption doesn't protect you, at least not completely
- Authentication doesn't protect you, at least not completely
- Firewalls?
- Why would anybody attack us?

MIS 5211.701 45

45

Leakage

- Signal required to use wireless access means you need to be relatively close
- Signal required to "sniff" traffic means attacker could be miles away with the right conditions

Venezuelans set new WiFi distance record: 237 miles

by Nilay Patel | | June 19th 2007 at 7:01 am

Source: http://www.engadget.com/2007/06/19/venezuelans-set-new-wifi-distance-record-237-miles/.

MIS 5211.701 46

46

Old Ways Are The Worst Ways

- Wireless networking is a shared segment
  - Think "Hub", not "Switch"
- Sniffing is passive
  - No access required
  - No forensic evidence attacker was there
  - Only need some level of physical proximity
- So, you would need to be here, to be safe. Maybe!

Source: http://www.darkgovernment.com/news/wp-content/uploads/2009/04/area-51-satellite-image.jpg

MIS 5211.701 47

47

Denial of Service

- RF Jamming
  - Expensive
  - Traceable
- 802.11 attacks
  - Cheap (Free?)
  - Can look like regular traffic
  - Effective, and hard to locate

MIS 5211.701 48

48

Protocol Issues

- Long history of problems
  - WEP
  - LEAP
  - Bluetooth authentication
  - Preferred networks broadcast
  - Management frames cannot be encrypted
    - Easily captured
  - Geo Location

MIS 5211.701 49

49

Standards

- Multiple players
  - FCC – Federal Communications Commission
  - IEEE – Institute of Electrical and Electronics Engineers
  - IETF – Internet Engineering Task Force
  - WiFi Alliance

MIS 5211.701 50

50

FCC

- Government Regulatory Body
  - Sets output power limits
  - Investigates interference cases
  - Requires acceptance testing of new products prior to going on sale
  - Covers all of US including territories

MIS 5211.701 51

51

IEEE

- Develops the detailed "specifications" for layer 1 and 2
  - PHY
  - MAC
- Complies with FCC and other country regulatory bodies
- Membership made up of vendors, manufactures, etc…

MIS 5211.701 52

52

IETF

- Similar makeup to IEEE
- Responsible for layer 3 and above
- Standards are published as RFCs

MIS 5211.701 53

53

WiFi Alliance

- Trade Organization
- Focused on interoperability
- In early days, worked out pre-specification requirements due to vendor concerns over time required by IEEE and IETF

MIS 5211.701 54

54

EAP

- Extensible Authentication Protocol
- Defines framework to authenticate users to the network (Not limited to Wireless)
- Works with IEEE 802.1x
- IETF provides extremely detailed information
  - http://tools.ietf.org/html/rfc3748

55

802.11i

- The replacement for WEP
- Provided for enhanced security
- Introduces TKIP and CCMP
  - TKIP – Temporal Key Interchange Protocol
  - CCMP - Counter Mode Cipher Block Chaining Message Authentication Code Protocol, Counter Mode CBC-MAC Protocol or simply CCMP
- Later rolled in to 802.11-2007

56

802.11 MAC Layer

- Definitions
  - "dB" – Decibels
  - SSID – Service Set Identifier (Name Advertised)
  - BSSID – Basic Service Set Identifier (Think MAC Address)
  - EAP Extensible Authentication Protocol
  - EAPOL – EAP over LAN

57

802.11 MAC Layer

- Basic access mechanism
- Fragmentation support
- Reliable data delivery
- Network separation on same frequency (BSSID)
- Mobility between BSSs (Roaming)
- Power Management

MIS 5211.701 58

58

Architectures

- Not just Access Points
  - Peer to Peer (Ad-Hoc)
  - Point to Point (Typically proprietary to bridge locations where cabling is not feasible, also known as Wireless Distribution Networks)
  - Mesh (Think massive ad-hoc)
  - Wireless Switches

MIS 5211.701 59

59

802.1x

- IEEE Specification for network authentication
- Originally designed for wired networks
- Used for NAC (Network Access Control)
- Requires
  - Supplicant (End point agent)
  - Authenticator (Typically a 802.1x capable switch)
  - Authentication Server (LDAP, AD, etc…)

MIS 5211.701 60

60

802.11 Framing

- 802.11-2007 defines MAC layer
- Three types of frames
  - Management (Beacon, Probe, Authentication)
  - Data
  - Control (Confirmation of packet reception)
- Defines addressing and features
- Designed to accommodate roaming, power management

MIS 5211.701 61

61

More Wireless Security

- Open WiFi Networks vs Encrypted WiFi Networks
  - In an open network, your browsing can be monitored
  - Everything is sent in the clear
  - WPA2-PSK fixes this "Somewhat"

MIS 5211.701 62

62

WPA2-PSK

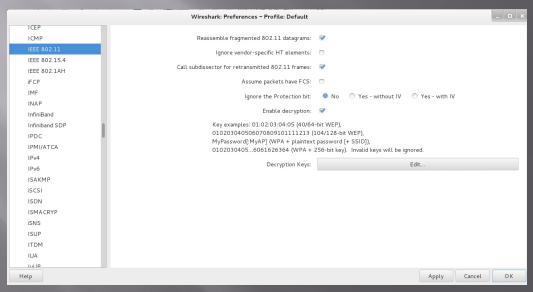
- Uses a pre-shared key (hence the acronym PSK)
  - The pre-shared key is known to all authorized users
  - Anyone with the pre-shared key has what they need to decrypt traffic
  - Wireshark has a built-in option to decrypt traffic if you have the key
  - This means WPA2-PSK is not much more secure than no encryption, unless you trust everyone on the network

MIS 5211.701 63

63

Wireshark WPA2-PSK Decryption

- Edit->Preferences->IEEE 802.11



64

PTK or Pairwise Transient Key

- WPA2-PSK tries to address this issue by use of PTK
- However, the PTK is derived from the PSK
- So… It is easy to capture the PTK if you have the PSK

65

WPA2-Enterprise

- WPA2-Enterprise corrects these issues for large networks
  - EAP authentication along with a Radius server ensures each client gets a unique key
  - Other authenticated users no longer have a master key to decrypt the traffic

66

WPA2 Hole196 Vulnerability

- Even in WPA2-Enterprise there is still a potential vulnerability from other authorized users (Abuses GTK or Group Temporal Key)
- Limited to:
  - ARP poisoning
  - Injecting malicious code
  - Denial of Service w/o using de-auth packets
- More detailed description
  - https://community.arubanetworks.com/t5/Community-Tribal-Knowledge-Base/Analysis-of-quot-Hole-196-quot-WPA2-Attack/ta-p/25382

MIS 5211.701 67

67

Key Reinstallation Attack

- Also known as KRACK
- **The attack works against all modern protected Wi-Fi networks**
- https://www.krackattacks.com
- Basically, takes advantage of weakness in protocol to reinstall keys

MIS 5211.701 68

68

Next Week

- More Wireless

MIS 5211.001 69

69

70