Lecture 2 - Cryptography

History of Cryptography

- Cryptography
  - Science of secret writing
  - Greek: Kryptos Graphia
  - Hiding what you are writing
- Cryptoanalysis
  - Science of breaking ciphers
- Cryptology
  - Encompasses both subjects

Ancient History

- Egypt 1900BC non-standard hieroglyphs
- Mesopotamian tablet 1500BC
- Hebrew scripts -> substitution cipher ATBASH (500-600BC)
- Greece 487BC -> skytale
- Caesar Cipher (50-60BC) -> substitution cipher with normal alphabet, shift n places to encode, shift a few more to decode
- 725-790AD Arabic mathematician wrote a book on Cryptography.
- Roger Bacon (1250AD) "A man is crazy who writes a secret in any other way than one which will conceal it from the vulgar"
- 1466-1467AD designing a cipher disk.
- 1518AD Johannes Trithemius wrote the first printed book on Cryptology. Invented a steganographic cipher in which each letter was represented as a word taken from a succession of columns.
- 1553AD Glovan Batista Belaso -> Vigenere cipher
- 1563AD Glovanni Battista Porta wrote a text on ciphers, introducing the diagraphic cipher.
- 1790AD Thomas Jefferson invented wheel cipher. Used in WW2
- 1854AD Charles Babbage reinvented wheel cipher.
- 1913AD Captain Parket Hitt reinvented wheel cipher.
- 1917AD Gilbert S. Vernam, invented practical polyalphabetic cipher machine capble of using a key which is totally random and never repeats.
- 1918AD The ADFGVX system was put into service by the germans in WW1.
- 1923AD Arthur Scherbius -> Enigma Machines
- 1927-1933AD American Prohibition -> "The greatest era of international smuggling -- prohibition -- created the greatest era of criminal cryptography"
- 1976 Introduce asynchronous encryption.
- 1977 Diffie-Hellman Key Exchange -> RSA created

- 1984-1985 ROT13 -> USENET News server software.
- 1991 Phil Zimmermann -> PGP (Pretty-good-privacy)
- 1994 The blowfish cipher is described by Bruce Schneier
- 1997 NIST looks to replace DES.
- 1998 AES standard evaluation.
- 1999 Rijndael chosen to be AES standard.

Perception of Encryption

- With the advent of ecommerce and the use of crypto in every day life the perceptions and needs have changed.
- Traditionally, encryption as used to prevent a third part gaining access to information in transit.

Definitions

- Plaintext
- Cipher text
- Crypto system -> a system that provides encryption and decryption
- Algorithm
- Key -> the random comppnent used to seed the encryption algo.
- Key space -> potential pool of possible keys
- Key clustering -> when >1 keys produce the same cipher text
- Work Factor -> how hard an algorithm is to break in terms of resources.

Keys - Questions to ask

- Choosing the right key is essential to any form of encryption?
- Where are the keys generated?
- How are the keys generate?
- Where are the keys stored?
- How do they get there?
- Where are they keys used?
- How do we replace a lost key?

Keyspace

It is a bad idea to have a small keyspace... more entropy === better

Classical Cipher Systems

- Substitution Ciphers

- One-time pad (Vernam Ciphers)
- Uses modulo addition
- Book / Running Key
    - Large body of text
    - Vulnerable to redundancy
- Codes
    - Construction of words/phrase mappings to other phrases, number of symbols.
- Stengography
    - From the greek for covered writing
    - Hiding the existence of a message
    - Microdots, watermarks.
- Encoding is not the same as enciphering.
- Encoding is when there is a symbol exchange. Usually involves a code book of some kind.

Symmetric Encryption

- Plaintext is encrypted using a secret key
- Ciphertext is decrypted using the same key.
- The process makes use of public and private compontents.
- Public
    - Algorithm to be used
    - The cipher text
- Private
    - The key to be used
    - The exact transformation used out of a number of possibilities.

Asymmetric Encryption

- Makes use of multiple keys for greater security, and solving the problem of key distribution
- Each part has their own keypair, obviating the need for a shared secret key
- Bases on the work by Diffie & Hellman Rivest, Shamir & Adleman
- Finding large prime factors of numbers is a problem.
- Some points to note
    - Public key cannot decrypt a message it encrypted
    - Ideally a private key cannot be derrived from a public key.

Strengths and Weakness

Asymmetric

- Strengths
  - Better key distribution
  - Scalability
  - Provides confidentially, authentication, non-repudiation
- Weaknesses
  - Slower and more resource intensive than symmetric systems.

Symmetric

- Strengths
  - Faster than asymmetric systems
  - Hard to break if sufficiently large systems
- Weaknesses
  - Key distribution
  - Scalability
  - Limited security
    - Confidentially only
    - No Authentication or non-repudiation

Goals of crypto

- Confidentially
- Authentication
- Integrity
- non-repudiation
  - Sender and Recipients cannot deny having sent or received a message

Maths

As long as we know XOR we're fine.

Properties of a Cipher

- Confusion
  - Strong keys cause confusion by introducing unknown values
- Diffusion
  - Plaintext input is put through mant functions and components are therefore dispersed.
- Reduced redundancy
- Fair statistical distribution

Are all ciphers the same?

- Different applications have needs for different ciphers, or ciphers operating in different mods.
- Block
    - Used for encrypting blocks of data such as files
- Stream
    - Operate one bit or character at a time, length of data unknown.

Block Ciphers

- Can be used for encryption and decryption purposes
- Messages are divided into blocks of bits.
- Each block is encrypted in parallel
- Makes use of confusion and diffusion
- Substitution-Boxes are often used
- Better suited to software implementations
- Some can operate in a stream cipher emulation mode.

Stream Ciphers

- Cipher operates on much smaller comonents of a message, usually bit or byte level.
- Uses a key stream and XOR with each bit as it comes in.

Hashing

- Reduction functions used to tranform a message of arbitrary length to a fixed length 'fingerprint'
- Based around a one-way function
    - y=F(x) is easy
    - x=F`(y) is not
- A crypto hash is a digital fingerprint for a message
- Reduces a large volume of input data down to a 'unique' array of bits.

- Ease of computation
- Compression -> fixed output
- Pre-image resistance
    - One way
    - Weak collision resistance
- Two flavours
    - One-Way OWHF

Goals

- Provides Integrity.

Lecture 3

Public Key Crypto

- Asymmetric Enc. is slow but is useful to encrypt symmetric keys.
- Symmetric key is fast but has the problem of distributing keys.

Sending a Message (PGP)

1. Alice writes a message
2. Alice generates a symmetric key
3. Alice encrypts message using symmetric key
4. Alice hashes the cipher text and signs it using her private key
5. Alice encrypts the symmetric key with the Bob's public key and sends him the entire message with signature, payload and encrypted symmetric key.
6. If Alice wants to send the same message to other people then she can simply encrypt the symmetric keys with their public keys and send the whole thing to them as well.

Public Key Infrastructure

- NOT PKC (not public key cryptography)
    - SMPT vs Email Infrastructure
    - SMTP does not provide all the different protocols and storage.
- Provides:
    - Authentication
    - Confidentially
    - Integrity
    - non-repudiation
- Hybrid Crypto Systems

Certificate Authorities

- CA is an organisation that maintains and issues public key certificates.
- CA is trusted by people to perform some kind of verification on clients.
- I trust you because the CA trusts you
- Should maintain a Certificate Revocation List (CRL)
- Work with registration authorities (RA)
- Multiple certificates for improved security.

PKI Gives us

- Confidentially
- Access Control
- Integrity
- Authentication
- Non-Repudiation

Digital Signatures

- Encrypt a hashed message with private key
  - RSA
  - DSA
- Hashing
- SHA2 & SHA3

Attacks on Hashing

- A hash function produces the same message digest for two different messages in a collision
- Observed collisions lessen the security of the cryptographic method.
- Similarly, it's very hard to create a message for a given digest.
- However, it's orders of magnitude easier to create two messages that share a hash.

Key Storage

- Keys are stored pre and post-distribution
- Where is a secure place to store a key?
- Traditionally you moved them in a locked box
- Now most distribution is via automated process over secure channels.

Good key practice

- Like passowrds, cryptographic keys require some care and feeding
- Keys should be periodically changed
  - Often forced through expiry
- Keys shoudld be verified, and expired
  - Security dictates the frequency
- The change and communication of that change be secure.

Management Principles

- Key length should be long enough to provide the necessary protection required
- Transmissions and storage sould be secure.
- Keys should be random, and utilise the full reach of the key-space
- Lifetime of a key should be related to the sensitivity of the data being protected
- The more frequent the use, the shorter the lifetime. Why?
- Keys should be backed up or Escrowed
    - Split key into M parts
    - Set N s.t. M>=N
    - Any N parts can recover the key.
    - #Meth
- Keys should be properly destroyed at end-of-life

Link vs. End-to-End

- Encryption can be implement a two levels
- Link
    - All data on comms path is encrypted.
    - Include all packet headers, payloads, trailers, etc.
    - Proivdes CIA to all
    - IPSEC

- End-to-End
    - Application layer, only payloads encrypted.
    - Headers and other addressing information still visible.
    - S/MIME

Link Layer

- Advantages
    - All data encrypted, users don't have to do anything

- Disadvantages
    - Data is decrypted and reencrypted at each node.

End-to-End

- Advantages
    - Protection from Start to Finish
    - User discretion / flexibility as to what gets encrypted, and how
    - Higher granularity due to increased keys
    - Messages not decrypted at each hop

- Disadvantages
    - Headers, addressing, routing info not protected -> leakage

    - Destination systems need appropriate config end-users.

Cracking Crypto

- Passive Attacks
    - Attacker is not affecting keys, protocol, algorithm used, or the messages being passed
    - Very hard to detect, and relatively easy to mount, impossible to detect.
        - Often a pre-cursor other things
    - Prevention rather than detection
    - Examples
        - Sniffing
        - Eavesdropping
        - Data capture and interception

- Active Attacks
    - Modification of file, data streams and masquerading as another party, attacker is actively involved.
    - Cipher text-only
    - Known-plaintext
    - Chosen-plaintext
    - Chosen-Cipher text
    - Main in the middle
    - Dictionary
    - Replay

Lecture 4

Identification

- Subjects claimed identity must be verified
- Two phases in identification
    - Public - claimed identity
    - Private - verification

- Can be based on three primary factors

    1. Something you know (Password)
    2. Something you have (Token)
    3. Something you are (Biometrics)

Better Passwords

- Cognitive Passwords
    - Fact or opinion based challenge response
    - Commonly used as a backup in the even of password loss. What is your dog's name?
- One-Time Password
    - A password that is generated systematically and only usable for a single instance

```
94: BEAT WHEE CORD RISK JOBS ...
95: ...
96: ...
```

Salty Passwords

- What is Salt?
- Why does salt improve things?
- Salt adds additional entropy to passwords.

What is a good password?

- Length beats complexity

Pass phrase

- Different from passwords
- Pass phrase is usually much longer and more complex
- More likely to remember because it makes sense
- Application takes a pass phrase and generates a 'virtual password' to be used in identity authentication.
    - e.g. `IlikeMyGreenEggsWithoutHam`

Tokens

- These are a physical piece of hardware
- Build on the One-Time Password
- Challenge Response-Based

- Require PIN entered and they ? time Synched OTP
- Other types store a digital certificate, and must be physically connected to a device (see U2F)

Biometrics

- Verification of an individual (human) identity based on a unique physiological aspect of their person.

Guest Lecture (DFIR)

Digital Forensics

- Incident ->
- Detected ->
- Identification (usually skipped by corporates) ->
- Remediation ->
- Report ->
- Incident -> and so on...

Identification

- Corporates usually skip identification due to the fact that they're paranoid.
- Remediation is usually a loud process that tips the fact that the breach has been detected and gives attackers a chance to change their modus operandi (MO).

Incident Response

- Used to demonstrate due dillegence to gov. agencies.

Digital Forensic Process

- Acquisition ->
- Examination ->
- Analysis ->

- Report

Memory is Important

- Memory contains things like keys for full-disk encryption.

Places to get data from

- User directory (all files that are created by the user)
- Registry (ties to user data)
- Windows Directory (sys32/config)
- See diagram

Analysis

- Reconstruct system activity over a period of time.

Lecture 5

Biometric Ranking

Effitiveness

- Palm scan
- Hand Geometry
- Iris scan
- Retina scan
- Fingerprint
- Voice print
- Facial scan
- Signature dynamics
- Keyboard dynamics

Acceptance

- Iris scan
- Keyboard dynamics
- Signature dynamics
- Voice print
- Facial scan
- Fingerprint
- Palm scan
- Hand Geometry
- Retina scan

Biometric Errors

- Type 1
    - False rejection rate
- Type 2
    - False acceptance rate
- Crossover Error Rate (CER)
    - Where FRR === FAR

Cryptographic Keys

- Strong public key enc. is used to generate key pairs
- Identity Authentication is based on them being a matching crypto key-pair.
- Commonly used protocols like SSH

Memory and smart cards

- Differ only in processing power on-board smartcard has a functional CPU
- Both have Memory
- Simplest form is an ATM card
- Smartcard can be used to provide secure authentication using a challenge-response
    - Home affairs use biometric and cryptographic keys on your ID card

Authorisation

- Different from authentication
- Authentication -> Verifying idenity
- Authorisation -> Validating that the subject is allowed to perform a specific action.

Access Criteria

- Access criteria should be as fine grained as possible
- Fine grained === huge complexity
- Access criteria are the rules used in the authorisation process
- Prevent 'access creep'
  - Revoking privilege is a real problem.
- Roles
  - Tied to a role that filled rather than a person
- Groups
  - Certain groups of people get permissions
- Physical/Logical location
  - It depends where you are
  - Geolocation is fairly accurate (at least to the country level)
- Time of Day (Environment)
  - Access only granted during specific hours
- Transaction Type
  - Certain classes of transaction may be granted and other forbidden

Principal of least access -> black and whitelisting

Reliable Defaults

- Know your default
  - Default allowed
  - Default deny
- Deny is safer as it catches anything not explicitly allowed
- Protocols against unforseen holes
- Know how your system process Access Control Rules
  - List based
  - Chain based

Least privilege

- Need to Know
    - If you don't need to know information in order to perform a task; information is withheld

Single Sign-On

Single Sign-on provides a single point of initial authentication, and this is then propagated.

- Scripts
- Kerberos
- SESAME
    - Secure European System for Applcations in a Multi-vendor Environment
- Thin clients
- Windows Domains

Access Control Models

- An ACM is a framework that dictates how a subject accesses objects
- Discretionary
    - User owns information they create
    - Ownership can be assigned
- Mandatory (MAC)
    - gives data owners some say in access to the data by others
    - The operating system has the final say in access control decisions
- Non-Discretionary
    - Also know as Role-based access control
    - Role-based or Task-based
    - Latice-Based
        - Determined by sensitivity level assigned to a Role
        - provision of an upper and lower sensitivity boundary

Access control admin

- All this access control comes with a cost (admin)
- Centralised
    - RADIUS
    - TACACS/TACACS+

- De-centralised/Distributed
    - Security Domains
- Hybrid
    - Federations (TRUST REQUIRED!!!)
    - Miracle that eduroam works
        - No real legal enforcement between parties

Security Domains

- A security domain is not a windows domain
- Subjects within share a common security policy, procedures and rules.
- Note this is slightly different to the Microsoft concept of a Network Domain
- Actual implementation of the doimain hierarchical.

Access Control Layers

- Physical
- Technical

Physical

- Network segregation
    - Physical split in network
- Perimeter security
    - Guard your borders
- Computer controls
    - Cable locks, drive locks -- even a lack of drives
- Work area separation
    - Restricted access separation of duties, need to know & least privilege.
- Data backups
    - Backup MUST happen -> secure, offsite and offline storage
        - RAID IS NOT A BACKUP SOLUTION
- Cabling
    - Prevention from damage, interception, theft
- Locks
    - ?

Technical

- System Access
- Network Architecture
- Network Access

Administrative

- Policies and Procedures
- Personnel controls
    - Separation of duties etc.

Access Control Types

- Layered Defence
    1. Perimeter Security
    2. Intrusion Detection
    3. Username and Password
    4. Access control lists
- Access controls can be classified as follows
    - Preventative
    - Detective
    - Corrective
    - Deterrent
        - Security cameras (if you know you're being watched then you're unlikely to do something wrong)
    - Recovery
        - Incident managment
    - Compensating
        - How do we fix things after incident?

Good practice

Keep the least number of doors and windows open and you'll keep the flies out.

- Minimum accounts
- etc.

Summary

- Access controls are your first line of defence. YOU NEED THIS.
- Critical to maintaining of system integrity and the CIA of the information contained within
- Controls can be of varying types
- One size does not fit all, org needs to find what works for them vs cost.

Lecture 6

Physical Security

- The physical protection of assets
- Assets may be tangible / intangible in nature
- Protection against:
    - Theft
    - Destruction
    - Damage
    - Interference

Threats

- Emergencies
    - Fire and smoke
    - Building/structure damage
    - Loss of power
    - Water damage
    - Toxic materials
- Natural Disaster
    - Earth movement
    - Storm Damage
- Human Factor
    - Sabotage
    - Vandalism
    - War
    - Strikes

The Big 7

- Temperature
    - Extreme variations
- Gasses
    - Military gas, commercial vapours, humidity, suspended particles.
- Liquids
    - Water and chemicals. Floods, cleaning fluids.
- Organisms
    - Viruses, bacteria, people, insects, animals
- Projectiles
    - Tangible objects in motion, and powered objects
- Movement
    - Collapse, sheering, shaking, vibration, liquefaction.
    - "If you shake something enough at the right frequency it will liquify"
- Energy anomalies
    - Surges or failures, static, noise, radiation

- Why we care about suspended particles?
    - Suspended particles such as flour dust are extremely flamable
    - Use copper fastenings to never have sparks.

Facilities Planning

Site Selection

- Visibility
    - What neighbours?
    - High enough security?
- Local Considerations
    - Crime rate?
    - Possible nearby hazards
- Natural Disasters
    - Likelihood of disaster?
- Transportation
    - Staff access
    - Excessive traffic
- Joint Tenancy
    - What are the terms, who has access to core services?
- External Services
    - Proximity of local emergency services

Site Design

We're more likely to be involved in this than Site Selection

- Walls
    - What is their construction
    - What is the fire rating?
- Ceilings
    - Weight bearing and fire rating
- Floors
    - Slab -> Weight rating, fire rating
    - Raised -> Fire rating, electostatics
- Windows
    - Should they be here?
    - Should filter light and be shatterproof/armoured
    - Burglar bars
- Doors
    - Resistance to forcible entry
    - Fire rating >= Walls
    - Safe state locks -> People **ALWAYS** take priority
- Sprinkler systems
    - Location and type should be suitable
- HVAC
    - Dedicated emergency power
    - Emergency shutoff
    - Positive air pressure
- Electrical
    - Backup power
    - Clean power
    - Secure operation and access

Audit Trails

- Like a computer system, physical location need audit trails
    - Date and time of access attempt
    - Was it successful?
    - Where was the access attempted
    - Who attempted access
    - who modified priviledges
- More of a detective measure than preventative.

Emergency Procedures

- Emergency plans need to be planned ahead of time and all staff trained in their execution
    - Emergency system shutdown procedures
    - Site Evacuation
    - Employee training and protection

Personnel Controls

- Commonly implemented by HR Dept.
- Pre-employment screening
    - Employment history, education, references.
    - Background and credit ratings where needed.
- On-going employee checks
    - Security clearances should be reviewed
    - Continuous employee rating/review
- Post-employment procedures
    - Exit Interviews
    - Return of organisation inventory
    - Removal of systems and physical access
- Reducing risk employees and company by employing people who are not succesptible to external influence.
    - Drug dealers
    - Gambling bookies
    - Debt
- None of the above are IT functions; however it still involves IT (revoking access control etc.)

Environmental & Life Safety Controls

- These controls are required to function correctly in order to sustain either the computer system's operating environment, or the personnel's environment
    - Electrical Power
    - Fire Detection & Suppression
    - Heating Ventilation and Air-conditioning (HVAC)
- Where there is conflict, people come first.

Electrical Noise

- Noise is bad...

- Radio Freq. Interference
- Generated by the components of an electrical system
    - Cables, Fluorescent lights
- Can cause damage to components
- Preventative measures
    - Power line conditioning
    - Proper grounding of systems
    - Shiedling
    - Limited exposure to and use of fluorescent lighting, heaters, magnets.

- Don't link buildings with copper cables.
    - Ground voltage differentials. -> Changes in "Ground" between buildings.

- Use fibre optics instead.

Static and Humidity

- Ideal -> 40%-60%

- High humidity can cause corrosion of parts and components -> silver migration in particular (in solder)
- Low humidity allows for statc build-up
    - 4000V on hardwood floor
    - 20kV on a carpet
- Relative humidity can be controled with HVAC

- Preventative

    - Anti-static sprays and flooring
    - Rooms should be grounded including floors
    - Anti-static matting, and leashes
    - HVAC humidity control.

Numbers

- 40V -> damage transistors and sensitive equipment

- 1000V -> Corrupt CRT monitor
- 1500V -> Data loss on disk drive

- 2000V -> etc.

Fire Detection and Suppression

- Successful suppression and detection of fire is essentially for continued operation, and

staff safety.

    - Class A
    - Class B
    - Class C
    - Class D+E -> Chemical Fire

- A fire is a case of rapid oxidisation of a material
- A fire requires: Heat, Oxygen, Fuel
- How can we suppress fires?
    - Class A -> Water
        - Reduce the temperature
    - Class A+B -> Soda Acid
        - Suppress Fuel Supply
    - Class B+C -> CO_2
        - Suppress oxygen
    - Class B+C -> Halon (and other gas suppressants)
        - Chemical reaction is used to supress fire, as well as replacing the oxygen.
- Use the right suppressant for the combustible.

- Heat-sensing
    - Based on either rate of change or a pre-determined temperature.
- Flame-actuated
    - Expensive, but accurate. Use a combination of Infra-red and ionisation sensors
- Smoke-actuted
    - Primarily used in ventilation systems, based of photoelectric systems

- Dial-up Alarm

    - When detection occurs an alarm can be sounded and emergency services summoned.

Physical Security Controls

- Guards

    - Oldest form of security surveillance
    - Have the advantage of decision making
    - Best resource dealing with personnel
    - Disadvantages
        - Availability
        - Reliability
        - Training
        - Cost
- Dogs
    - Loyal and effective
- Fencing

    - Primary boundary access control
    - Can provide channeling of traffic
- Lighting
    - Common use
    - Increases visibility
    - Critical buildings -> "8' high with 2' candle power"
    - Sometimes area illuminated in Infra-red
- Locks
    - Ancient access control method
    - Preset Locks
        - Use a physical key
    - Programable locks
        - Use a key press sequence or push buttons and may be reprogrammed.
- CCTV
    - Detective Control, used to enhance guard ability.
    - Also used in investigation and prosecution.
- Access Cards
    - Contain ID and access info
    - Magstripe incorporate into photo ID
    - May be used as token for access control.
    - Wireless proximity readers
        - No physical contact needed
            - Passive devices
            - Field-powered
            - Transponders
    - Biometrics

Intrusion Detection

- Perimeter Intrusion Detection
    - Photoelectric sensors
    - Dry Contact Switches / Metallic Tape
- Motion detection
    - Wave Patterns

Computer inventory

- Computers must be protected.
    - What happens WHEN you lose a phone or laptop
- Cable locks
- Port Controls

- Switch Controls
- Peripheral Switch Controls
- Electronic Security Controls

Media Disposal

- Magnetic media is persistent, and requires proper erasure
    - Clearing
        - Overwriting of data. Media intended to be reused in organisation
    - Purging
        - Degaussing and overwriting of media prior to removal from a secure environment.
    - Destruction

Common Faults

- Deleting a file does not erase it, FAT entries are simply updated.
- Damaged / 'bad' sectors on disks will generally not be formatted.
- Overwriting files may not destroy everything due to slack space.
- Degaussing equipment or operator failure.
- Media not formatted sufficiently -> DoD recommends destructive formats for sensitive media.

Summary

- Physical security is important as it usually provides the first line of defence in a layered protection strategy.
- Broad scope relating to protection of human and physical assets
- In any situation, people come first.