Threats To Communication

MSc in Information Security & Digital Forensics.

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

In This Section

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Lessons From History

- History tells us that the confidentiality of data is a much sought after property of a communications system.

- In the battle of the pacific, the Japanese never succeeded in breaking a major American code, and their inability to do so convinced them that their own codes were secure.

- The British and American forces were also arrogant about there own communications. As a result, both lost many men and ships.

- Even the ***Hotline*** between Churchill and Roosevelt was tapped.

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Lessons From History

When considering the security of any communications medium, there is a fundamental question to ask before any steps can be taken to analyse and implement security tools. That question is:

What is the value of my secrets or the information that I rely upon for my comfort or existence, and what are the consequences of its loss?"

There are as many degrees of threat as there are of solutions to those threats, but the answer to our question is the guide to what lengths should be taken to secure the user's position.

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Levels of Security

Generally speaking, there are three levels of information security:

- ***Personal security***
- ***Commercial security*** involving financial transactions and trade
- ***High security***, which encompasses national security, i.e. political and military security

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Threats to Communication

- *Eavesdropping*
- *Modification*
- *Replay*
- *Masquerading*
- *Repudiation*
- *Access*

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Threats to Communication

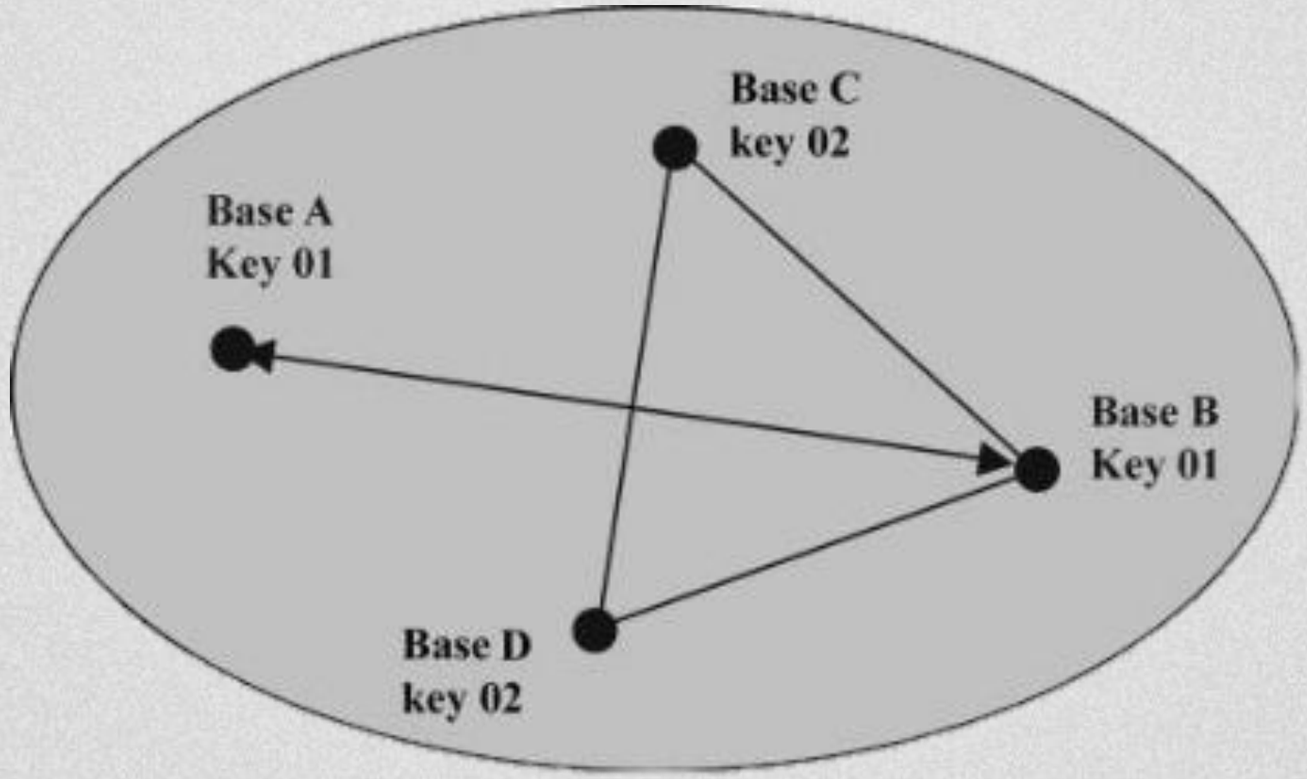
The cryptographic countermeasures or ‘security Mechanisms’ used to meet these threats are classified as:

- **Authentication**
- **Confidentiality**
- **Integrity**
- **Access**

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Authentication

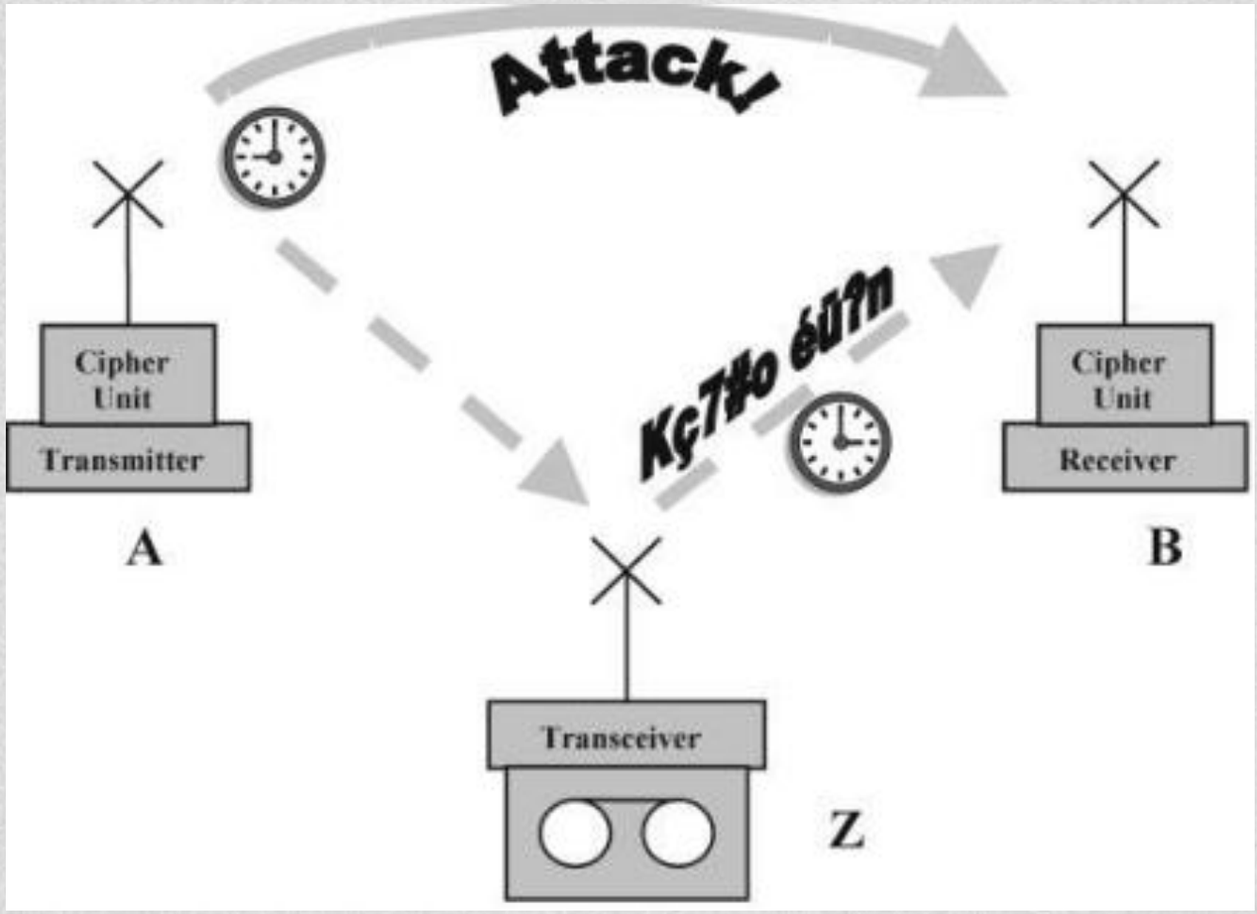
- Is the message coming from the purported source?
- This problem can be largely overcome by encryption and suitable key management.



Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Authentication

- There is a loophole, however, which may be exploited and that is the ploy of ***replay*** or ***spoofing***



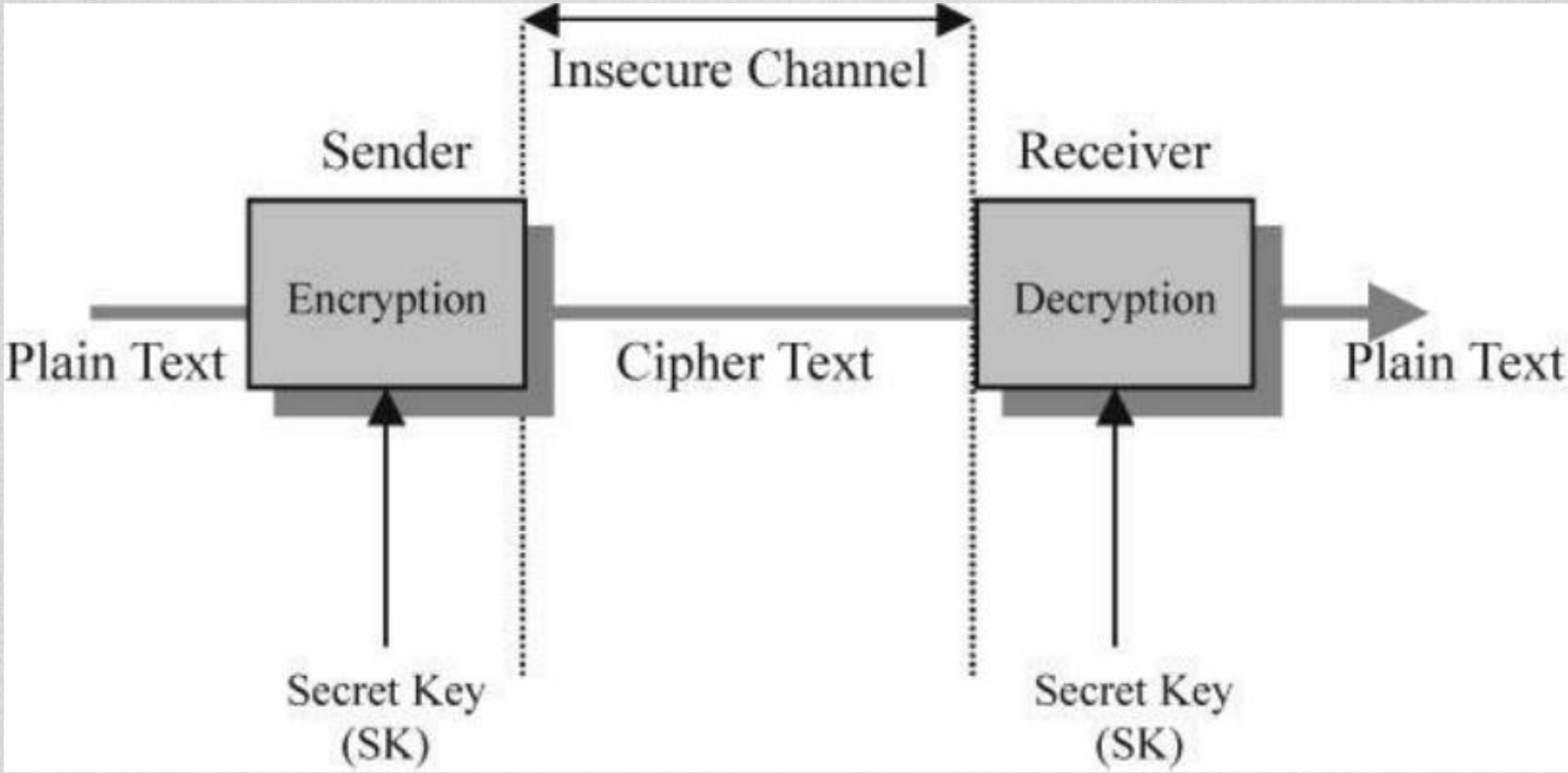
Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Confidentiality

- The confidentiality of a message, voice, text or data is assured by ***encryption*** with a ***secret key***.
- The secret key (SK) in a ***symmetric*** system is common to both sender and receiver.
- With an ***asymmetrical*** system each party has their own personal ***public*** and ***private*** keys. So, the keys are not common to both parties.

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Confidentiality



Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Integrity

- Messages and files need to be protected against modification, and whilst confidentiality procedures protect against eavesdroppers, they give little protection against modification and the integrity of the message or file.

- The solution to integrity threats is to employ ***digital signatures, MACs*** or some other redundancy scheme in the plain text and then use encryption.

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Digital Signatures

- These are asymmetric encryption tools that allow the author of the original message to ***sign*** their document in such a manner that the receiver can verify that what they receive is a faithful copy of the author's original.
- If, during the transmission through an unsecured medium or channel, the message has been tampered with, the verification performed by the receiver will give the output ***Invalid Signature***.

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Integrity

Digital Signatures offer:

- ***Public verifiability:*** where anybody in possession of the authentic public key can verify the signature
- ***Authenticity and integrity:*** as modification of a message or replacement can be detected
- ***Non-repudiation:*** the signatory of a message cannot deny having signed the document

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Digital Signatures

- *The purpose of the digital signature is just to check the message integrity. It is not used to encrypt the message and therefore does not offer confidentiality.*
- *However, combining the two techniques, where symmetrical encryption of the message text ensures confidentiality and with signature verification, by public key techniques ensuring message integrity, a hybrid system is produced. The result is a very powerful tool in protecting files and messages.*

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Availability

- *One of the more basic, yet essential, fundamentals in communications security is the control of availability and of access to the medium, sensitive data and ciphering equipment.*
- *The subject of physical access to the premises containing these entities is an important issue.*

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

PINs and Passwords

- The purpose of a password and PIN system is to authenticate users and facilitate their right of entry to whatever functions they are permitted to employ.
- In principle, it is a simple and basic method of controlling access

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Availability

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

PINs and Passwords

- PIN and password access is best controlled by adopting a policy of central command, whereby the central body controls all passwords and PINs from their generation, through use, enforced changes and eventual destruction.

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Guidelines for Password Use

- Passwords should be centrally controlled wherever possible but, in any case, should follow the guidelines below in order to add strength to access security:

  - Should be kept absolutely secret and not divulged to any other user

  - Should not be written down or recorded where they can be accessed by other users

  - Must be changed if there is the slightest indication or suspicion that a password has been compromised

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Guidelines for Password Use

- Must be changed when a member of the organisation leaves the group or changes their task
- Should use a minimum of six alphanumeric characters
- Must be changed monthly or at least bi-monthly.
- Must be changed more frequently the greater the risk or more sensitive the assets they protect
- Must not be included in an automated log in procedure, i.e. not stored in a macro function

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Availability

- **Biometric Access Tools**
- **Challenge / Response Control**
- **Tamperproof Modules**
- **Tempest Threats**

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

- **Tempest Threats (Van Eck phreaking)**
  The radiation emitted by all communications equipment and its security attachments. The term, tempest was coined by the US government to identify the problem of compromising radiations. It is used as a standard of protection against electronic hardware electromagnetic radiation.

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Thank You !

End of Section

Mark Cummins
Institute of Technology Blanchardstwon
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie