Security Engineering

Spring 2010

Dr. Marenglen Biba

General Info

- **Course : Security Engineering (4 credit)**
- **Instructor : Dr. Marenglen Biba**
- **Office : Faculty building 1st floor**
- **Office Hours : Tuesday 15-17 PM or by appointment**
- **Phone : 42273056 / ext. 112**
- **E-mail : marenglenbiba@unyt.edu.al**
- **Course page: http://www.marenglenbiba.net/seceng/**
- **Course Location and Time**
- **Laboratory Room 5A, Thursday 15-19.**

Purpose

- The goal of this class is to introduce students to engineering techniques for developing secure systems.
- The course will provide an introduction to security design and implementation with a focus on cryptography, security protocols and access control.
- It will provide a solid foundation for IT professionals/academics interested in the theory and practice of administration of complex scenarios involving security in computer systems.

Content

- Introduction to Security Engineering
- Access Control
- Cryptography
- Cryptographic Protocols
- Cryptographic Techniques
- Cryptographic Algorithms
- Multilevel Security
- Multilateral Security
- Secure Systems and Applications
- Design and Implementation

Required Readings

- Ross J. Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley | ISBN: 0471389226 Second Edition. (**required**).
- Schneier Bruce. *Applied Cryptography: Protocols, Algorithms and Source Code in C, Second Edition*, , John Wiley & Sons, Inc., 1995 (2nd edition), ISBN: 0-471-11709-9. (**required**)
- Handbook of Applied Cryptography Alfred Menezes (Editor), Paul van Oorschot (Editor), Scott Vanstone. CRC Press ISBN: 0-8493-8523-7, October 1996, (**recommended**).
- Matt Bishop. *Computer Security: Art and Science*. Publisher Addison Wesley, ISBN 0-201-44099-7, 2002. (**recommended**)

The 1st Book

- Ross J. Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley | ISBN: 0471389226 Second Edition. (**required**).
- The purpose of the book is to give a solid introduction to security engineering, as we understand it at the beginning of the twenty-first century.
- Ross Anderson
  - http://www.cl.cam.ac.uk/~rja14/

The 2nd Book

- The purpose of the book is to give a solid introduction to cryptography.
- Schneier Bruce. *Applied Cryptography: Protocols, Algorithms and Source Code in C, Second Edition*, , John Wiley & Sons, Inc., 1995 (2nd edition), ISBN: 0-471-11709-9. (**required**)
- Schneier Bruce
  - http://www.schneier.com/

Grading

- Midterm 35%
- Final Exam 35%
- Project 30%

- Internet use is necessary since students should regularly check the course home page.
- Continued and regular use of e-mail is expected
- Students must keep copies of all assignments and projects sent by e-mail.

Recommendations

- Start studying now
- The professor is a container of knowledge and the goal is to get most of him, thus come and talk.
- Respect the deadlines
- Respect the appointments
- Try to study from more than one source, Internet is great!
- If you have any problems come and talk with me in advance so that we can find an appropriate solution

GOOD LUCK AND HAVE FUN!

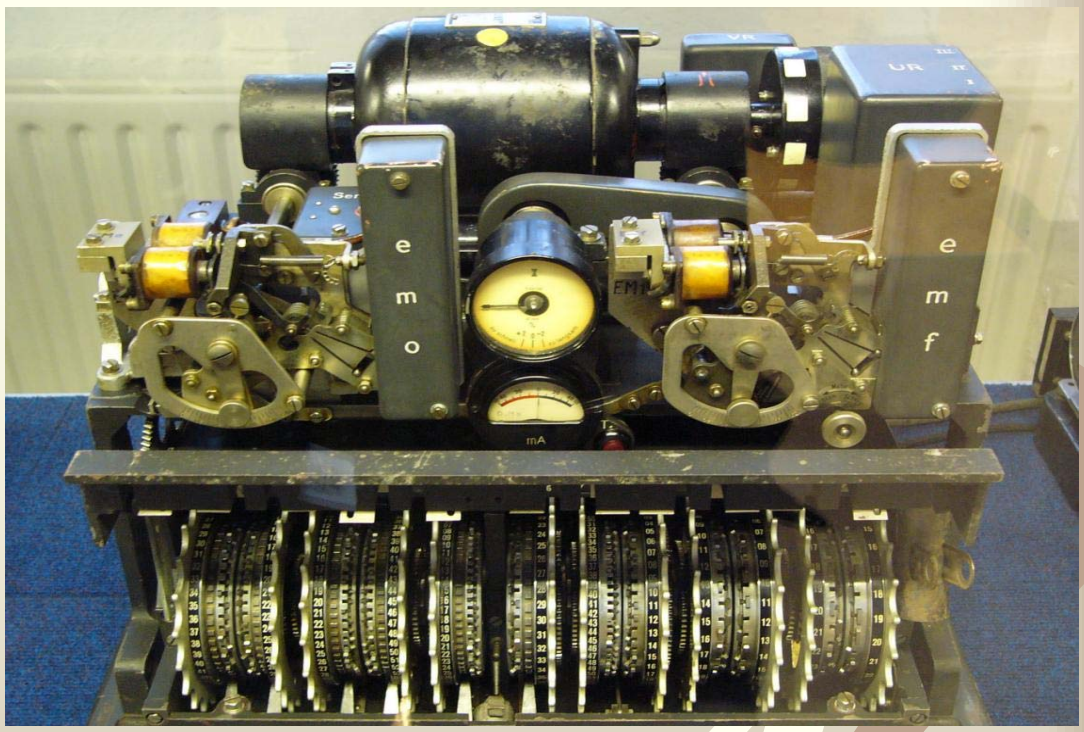
Lesson 0: History

Lorenz cipher

- The Lorenz SZ 40 and SZ 42 (Schlüsselzusatz, meaning "cipher attachment") were German cipher machines used during World War II for teleprinter circuits.

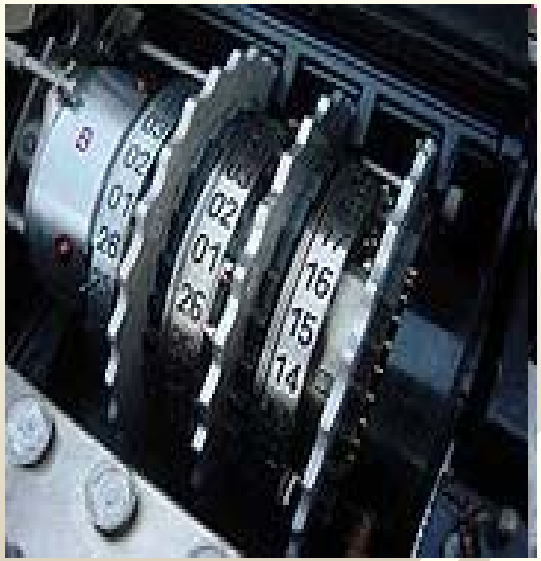
- British codebreakers, who referred to encrypted German teleprinter traffic as "Fish", termed the machine and its traffic "Tunny".

- While the well-known Enigma machine was generally used by field units, the Lorenz machine was used for high-level communications which could support the heavy machine, teletypewriter and attendant fixed circuits.



Enigma

An **Enigma machine** is any of a family of related electro-mechanical rotor machines used for the encryption and decryption of secret messages. The first Enigma was invented by German engineer Arthur Scherbius at the end of World War I.



The Enigma rotor assembly. In the Wehrmacht Enigma variant, the three installed movable rotors are sandwiched between two fixed wheels: the entry wheel on the right and the reflector (here marked "B") on the left.

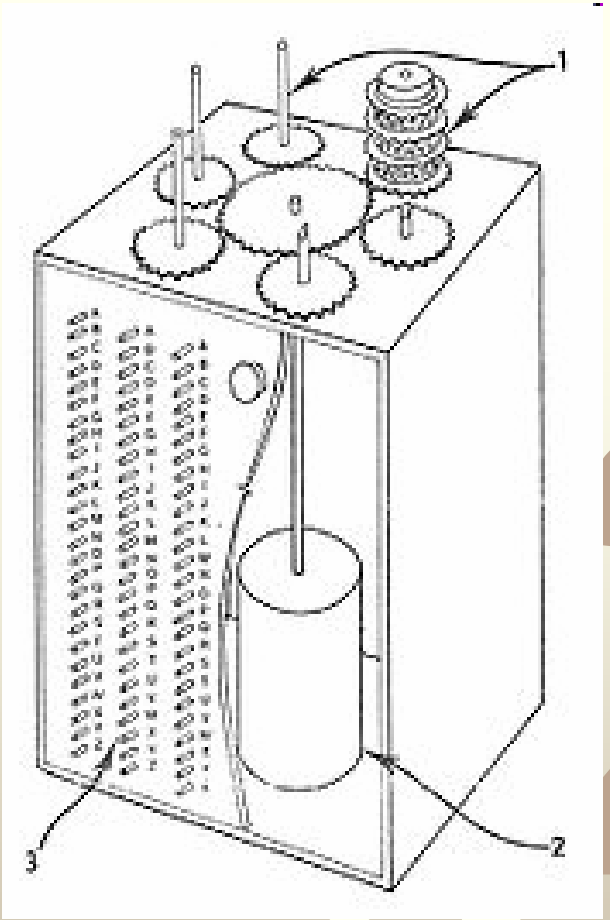
Enigma

The plugboard, keyboard, lamps, and finger-wheels of the rotors emerging from the inner lid of a three-rotor German military Enigma machine

Enigma in use, 1943

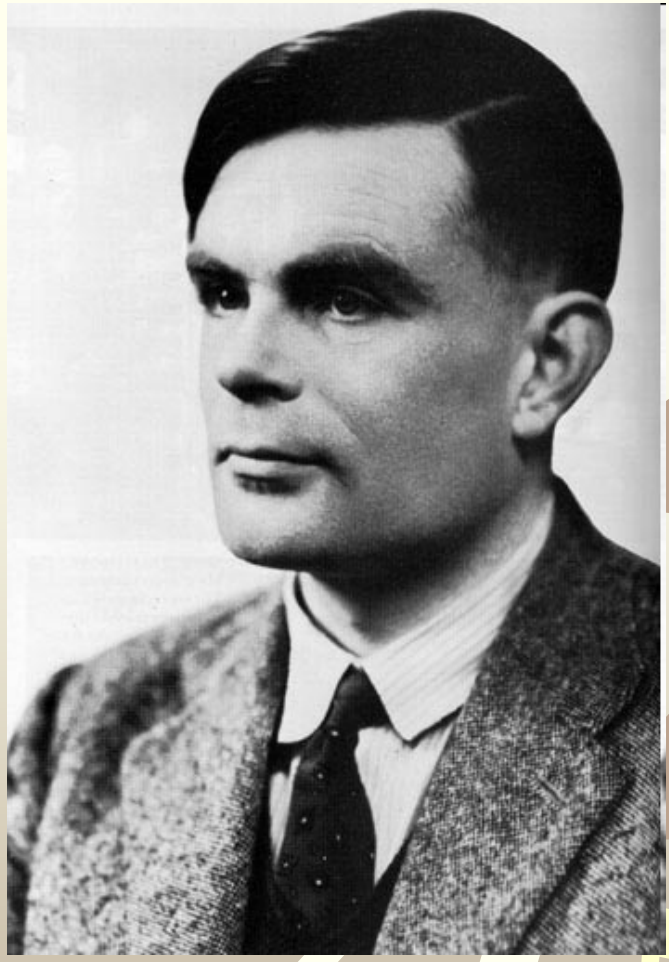
Bomba

- The bomba, or bomba kryptologiczna (Polish for "bomb" or "cryptologic bomb") was a special-purpose machine designed about October 1938 by Polish Cipher Bureau cryptologist Marian Rejewski to break German Enigma-machine ciphers.



Alan Turing (father of Computer Science)

- Alan Mathison Turing, (23 June 1912 – 7 June 1954), was an English mathematician, logician, cryptanalyst, and computer scientist.
- He was influential in the development of computer science and provided an influential formalisation of the concept of the algorithm and computation with the Turing machine.
- **In 1999 Time Magazine named Turing as one of the 100 Most Important People of the 20th Century for his role in the creation of the modern computer.**
- His Turing test was a significant and characteristically provocative contribution to the debate regarding artificial intelligence.



Turing: the first codebreaking machines

- During the Second World War, Turing worked for the Government Code and Cypher School at Bletchley Park, Britain's codebreaking centre.
- For a time he was head of **Hut 8**, the section responsible for German naval cryptanalysis.
- He devised a number of techniques for **breaking German ciphers**, including the method of **the bombe, an electromechanical machine** that could find settings for the Enigma machine.
- After the war he worked at the National Physical Laboratory, where he created one of the first designs for a stored-program computer, the ACE.

Turing–Welchman bombe

- Within weeks of arriving at Bletchley Park Turing had designed an electromechanical machine which could help break Enigma faster than bomba from 1932, the bombe, named after and building upon the original Polish-designed bomba.

- The bombe, with an enhancement suggested by mathematician Gordon Welchman, became one of the primary tools, and the major automated one, used to attack Enigma-protected message traffic.

Replica of a bombe machine

ULTRA

- Ultra (sometimes capitalised ULTRA) was the name used by the British for intelligence resulting from decryption of encrypted German radio communications in World War II.

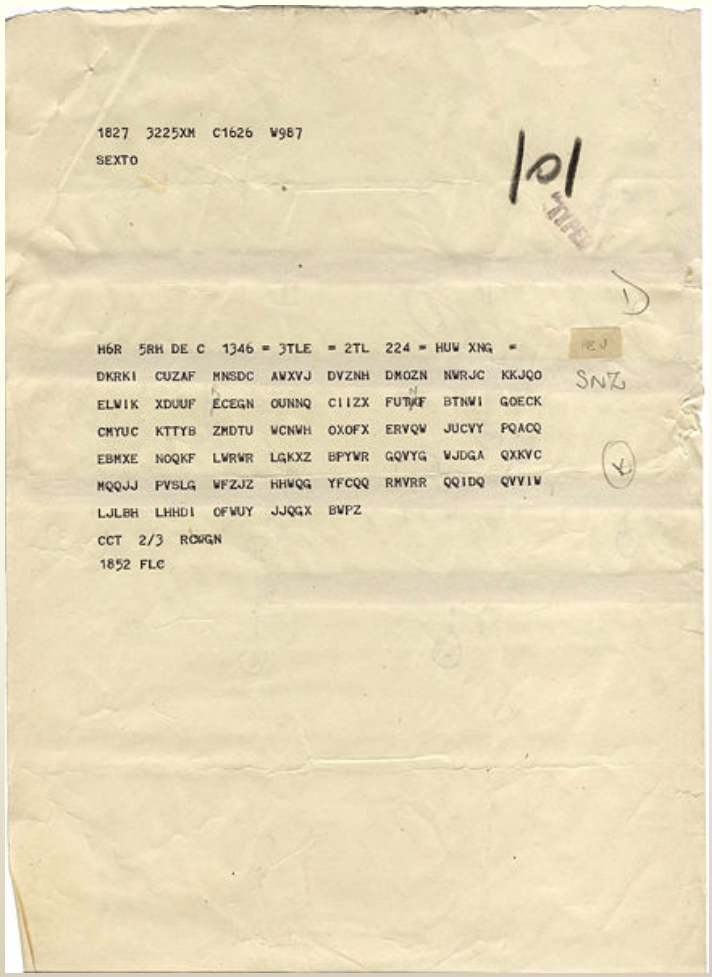
- The term eventually became the standard designation in both Britain and the United States for all intelligence from high-level cryptanalytic sources.

- The name arose because the code-breaking success was considered more important than the highest security classification available at the time (Most Secret) and so was regarded as being Ultra secret.

- Much of the German cipher traffic was encrypted on the Enigma machine, hence the term "Ultra" has often been used almost synonymously with "Enigma decrypts".

- However, in terms of the intelligence value, Lorenz SZ 40/42 decrypts were more important.

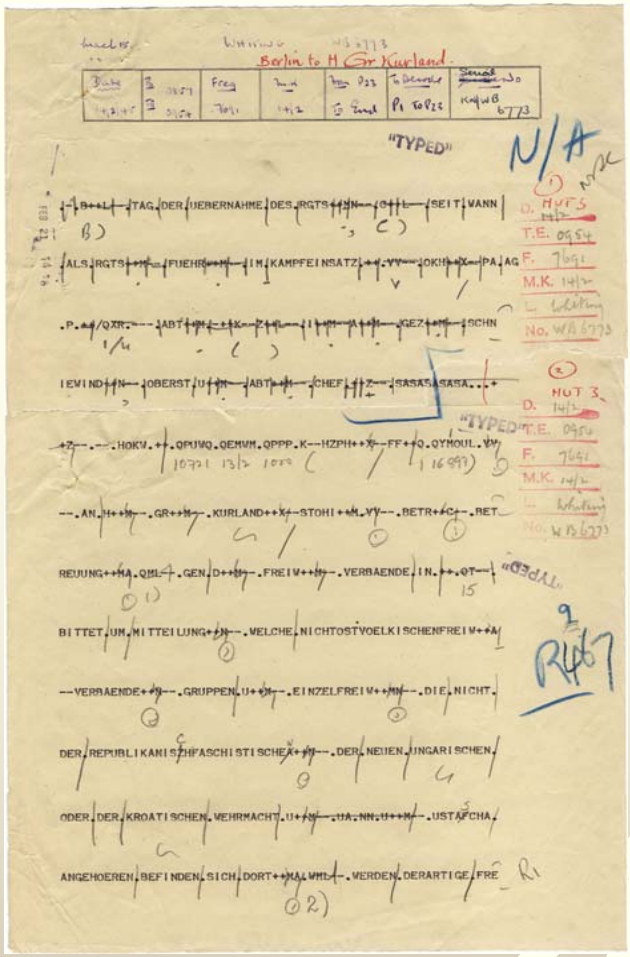
Deciphering documents with ULTRA: WWII



1827 3225XM C1626 W987
SEXTO

101

H6R 5RH DE C 1346 = 3TLE = 2TL 224 = HUW XNG =
DKRKI CUZAF MNSDC AWXVJ DVZNH DMOZN NWRJC KKJQO
ELWIK XDUUF ECEGN OUNNQ CIIZX FUTWF BTNWI GOECK
CMYUC KTTYB ZMDTU WCNWH OXOFX ERVQW JUCVY PQACQ
EBMXE NOQKF LWRWR LGKXZ BPYWR GQVYG WJDGA QXKVC
MQQJJ PVSLG WFZJZ HHWQG YFCQQ RMVRR QQIDQ QVVIW
LJLBH LHHDI OFWUY JJQGX BWPZ
CCT 2/3 ROWGN
1852 FLC



Berlin to H Gr Kurland

"TYPED"

N/A

TAG DER UEBERNAHME DES RGTS SEIT WANN

ALS RGTS FUEHR IM KAMPFEINSATZ VV OKH PA AG

.P. QXN. ABT K I A GEZ SCHN

IEWIND OBERST U ABT CHEF SASA SASA

HOKV. QPUWQ.QEMVM.QPPP.K HZPH FF O.QYMOUL.VV

.AN. GR .KURLAND STOHI .VV .BETR .RET

REUUNG MA.QML .GEN.D .FREIW .VERBAENDE IN. OT

BITTET.UM.MITTEILUNG .WELCHE.NICHTOSTVOELKISCHENFREIW MA

VERBAENDE .GRUPPEN.U .EINZELFREIW .DIE.NICHT.

DER.REPUBLIKANISCHFASCHISTISCHEX .DER.NEUEN.UNGARISCHEN.

ODER.DER.KROATISCHEN.WEHRMACHT.U .HA.NN.U .USTASCHA.

ANGEHOEREN.BEFINDEN.SICH.DORT MA.WMD .VERDEN.DERARTIGE.FRE

"TYPED"

Coded document

Deciphered document

F.W. Winterbotham, in *The Ultra Secret* (1974), quotes the western Supreme Allied Commander, Dwight D. Eisenhower, as at war's end describing Ultra as having been "decisive" to Allied victory in World War II.

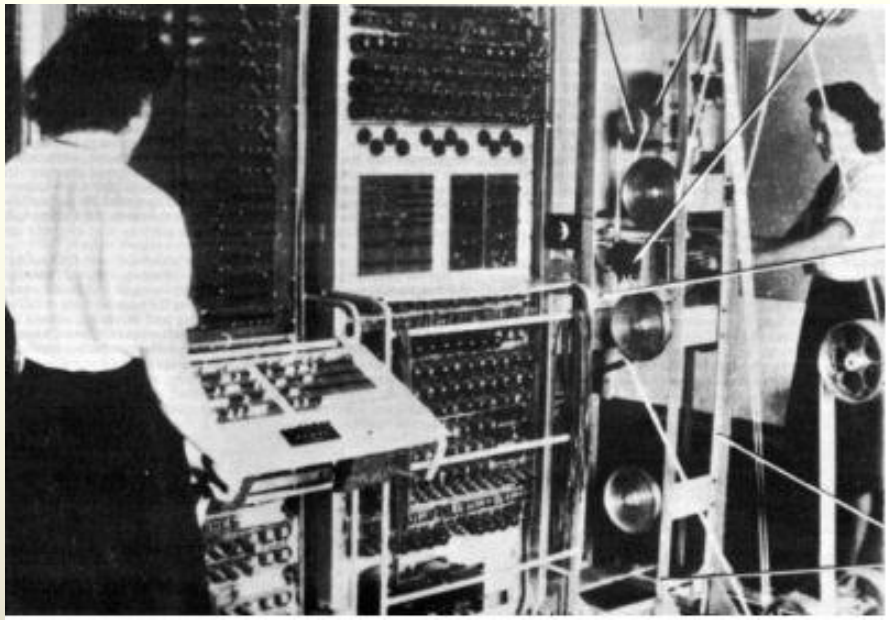
The birth of Colossus

- In July 1942, Turing devised a technique termed ***Turingismus*** or ***Turingery*** for use against the Lorenz cipher used in the Germans' new Geheimschreiber machine ("secret writer") which was one of those codenamed "Fish".

- He also introduced the Fish team to Tommy Flowers who, under the guidance of Max Newman, went on to build the Colossus computer, the **world's first programmable digital electronic computer**, which replaced simpler prior machines (including the "Heath Robinson") and whose superior speed allowed the brute-force decryption techniques to be applied usefully to the **daily-changing cyphers**.

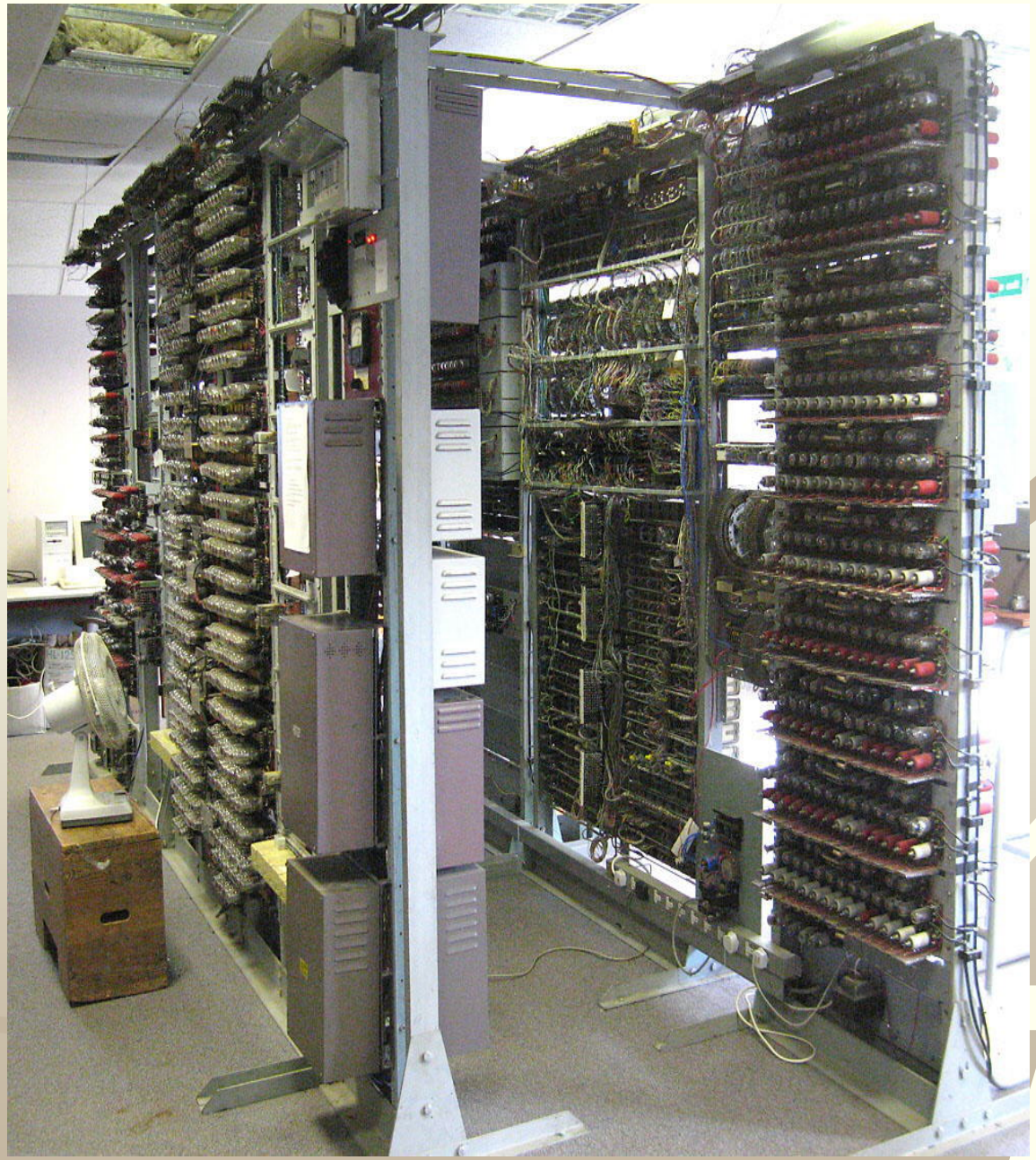
- A frequent misconception is that Turing was a key figure in the design of Colossus; this was not the case. While working at Bletchley, Turing, a talented long-distance runner, occasionally ran the 40 miles to London when he was needed for high-level meetings

Colossus – Mark I



COLOSSUS - Top-secret vacuum tube computer designed to break the Lorenz SZ40 (a relative of the Enigma) intercepted cyphers. This was a single purpose computer programmed cables and plugboards. Bletchley Park, Britain (1943)

Colossus rebuilt



Lesson 1

0011

Introduction to Security Engineering

Security: the past

- For generations, people have defined and protected their property and their privacy using locks, fences, signatures, seals, account books, and meters.

- These have been supported by a host of social constructs ranging from international treaties through national laws to manners and customs.

Security: the present

- Now most records are electronic, from bank accounts to registers of real property; and transactions are increasingly electronic, as shopping moves to the Internet.
- Just as important, but less obvious, are the many everyday systems that have been quietly automated.
  - **Burglar alarms** no longer wake up the neighborhood, but send silent messages to the police
  - students no longer fill their dormitory washers and dryers with coins, but credit them using a **smartcard** they recharge at the college bookstore;
  - locks are no longer simple mechanical affairs, but are operated by **electronic remote controls** or **swipe cards**; and instead of renting videocassettes, millions of people get their movies from satellite or cable channels.
  - Even the banknote is no longer just ink on paper, but may contain **digital watermarks** that enable many forgeries to be detected by machine.

How good is security tech?

- How good is all this new security technology?
  - Unfortunately, the honest answer is "**nowhere near as good as it should be**."
- New systems are often rapidly broken, and the same elementary mistakes are repeated in one application after another.
- It often takes four or five attempts to get a security design right, and that is far too many.

Security: growing threats

- The media regularly report security breaches on the Internet;
- Banks fight their customers over "**phantom withdrawals**" from cash machines;
- VISA reports huge increases in the number of disputed Internet **credit card transactions**;
- Satellite TV companies pursue pirates who **copy their smartcards**;
  - Law enforcement agencies try to stake out territory in cyberspace with laws controlling the use of encryption.

Failing and Working Systems

- As well as the systems that fail, many systems just don't work well enough.
- **Medical record systems** don't let doctors share personal health information as they would like, but still don't protect it against inquisitive private eyes.
- **Zillion-dollar military systems** prevent anyone without a "top secret" clearance from getting at intelligence data, but are often designed so that almost everyone **needs this clearance to do any work**.
- **Passenger ticket systems** are designed to prevent customers cheating, but when trustbusters break up the railroad, they cannot stop the new rail companies cheating each other.

Security Engineering: a new discipline

- Security engineering is the **new discipline** that is starting to emerge out of all this chaos.
- Although most of the **underlying technologies** (cryptology, software reliability, tamper resistance, security printing, auditing, etc.) are relatively well understood, the knowledge and experience of how to apply them effectively is much scarcer.
- And since the move **from mechanical to digital** mechanisms is happening everywhere at once, there just has not been time for the lessons learned to spread through the engineering community.
- **Time and again, we see the same old square wheels being reinvented.**

What is Security Engineering?

- Security engineering is about building systems to remain dependable in the face of malice, error, or mischance.
- As a discipline, it focuses on the tools, processes, and methods needed to design, implement, and test complete systems, and to adapt existing systems as their environment evolves.

Security vs Dependability

- Dependability = reliability + security
- Reliability and security are often strongly correlated in practice
- But malice is different from error!
  - Reliability: “Bob will be able to read this file”
  - Security: “The Chinese Government won’t be able to read this file”
- Proving a negative can be much harder …

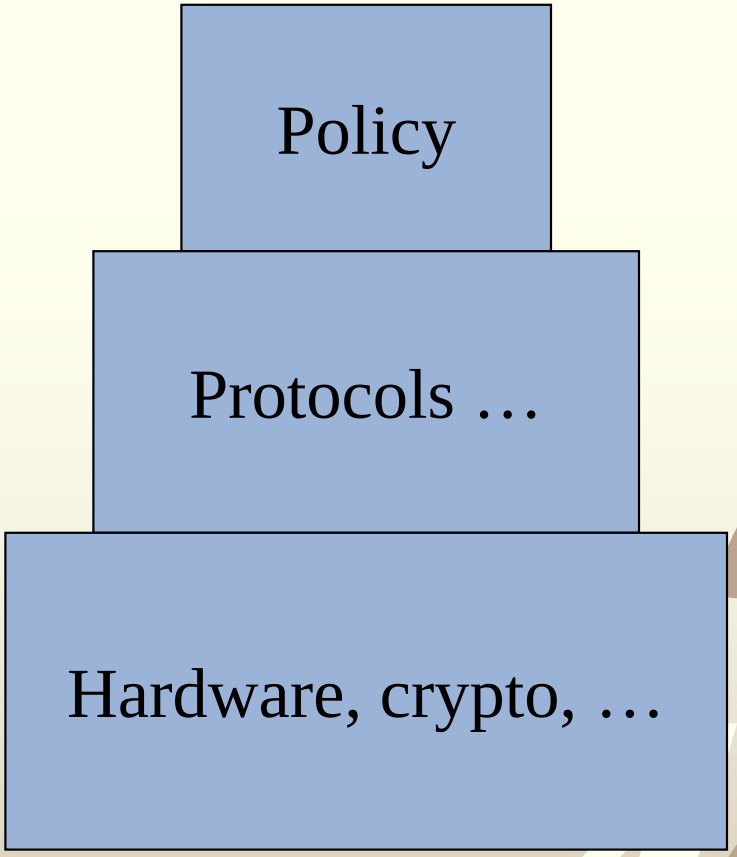
Building Security

- **Policy** (what should be protected)
- **Mechanisms** (cryptography, electrical engineering, …)
- **Attacks** (malicious code, protocol failure …)
- **Assurance –** how do we know when we're done?

- **How do we make this into a proper engineering discipline?**

Design Hierarchy

- What are we trying to do?
- How?
- With what?



Security engineering: cross-disciplinary

- Security engineering requires cross-disciplinary expertise, ranging from **cryptography** and **computer security** through **hardware tamper-resistance** and formal methods to a knowledge of **applied psychology**, organizational and audit methods and the law.
- System engineering skills, from business process analysis through **software engineering** to evaluation and testing, are also important; but they are not sufficient, as they deal only with error and mischance rather than malice.

Critical requirements

- Many security systems have **critical assurance** requirements.
- Their failure may:
  - **endanger human life** and the environment (as with nuclear safety and control systems),
  - **do serious damage** to major economic infrastructure (cash machines and other bank systems),
  - **endanger personal privacy** (medical record systems),
  - **undermine the viability** of whole business sectors (pay-TV)
  - **facilitate crime** (burglar and car alarms).
- Even the perception that a system is more vulnerable than it really is (as with paying with a credit card over the Internet) can significantly hold up economic development.

Sec. Eng Vs Soft. Eng

- The conventional view is that while software engineering is about ensuring that certain things happen ("John can read this file"), security is about ensuring that they don't ("The Chinese government can't read this file"). ☺
- Reality is much more complex.
  - Security requirements **differ greatly** from one system to another.
- One typically needs some combination of user authentication, transaction integrity and accountability, fault tolerance, message secrecy, and covertness.
  - But many systems fail because their designers **protect the wrong things**, or protect the right things but **in the wrong way**.

Bank: Bookkeeping

- *The core of a bank's operations is usually a branch bookkeeping system.*
- This keeps customer account master files plus a number of journals that record the day's transactions.
- The main threat to this system is the bank's own staff ☺
  - about one percent of bankers are fired each year, mostly for petty dishonesty (the average theft is only a few thousand dollars).

Bank: Bookkeeping

- The **main defense** comes from bookkeeping procedures that have evolved over centuries.
  - For example, each debit against one account **must be matched by an equal** and opposite credit against another; so money can only be moved within a bank, never created or destroyed.

- In addition, large transfers of money might need two or three people to **authorize** them.

- There are also alarm systems that look for **unusual volumes** or patterns of transactions, and staff are required to take **regular vacations** during which they have no access to the bank's premises or systems.

Bank: ATM

- *The public face of the bank is its automatic teller machines.*
- **Authenticating transactions** based on a customer's card and personal identification number— in such a way as to defend against both outside and inside **attack—is harder than it looks!**
- There have been many local epidemics of "**phantom withdrawals**" when villains (or bank staff) have found and exploited holes in the system.
- Automatic teller machines are also interesting as they were the first **large-scale commercial use of cryptography**, and they helped establish a number of crypto standards.

Bank: Messaging systems

- *Behind the scenes are a number of high-value messaging systems.*
- These are used to:
  - move large sums of money (whether between local banks or between banks internationally);
  - trade in securities; to issue letters of credit and guarantees; and so on.
- An attack on such a system is the dream of the **sophisticated white-collar criminal**.
- The defense is a mixture of :
  - **bookkeeping procedures**
  - **access controls**
  - **cryptography**

Bank: Strongroom

- Most bank branches still have a large safe or strongroom, whose burglar alarms are in **constant communication** with a security company's control center.

- **Cryptography** is used to prevent a robber manipulating the communications and making the alarm appear to say "all's well" when it isn't.

Bank: Internet

- *Over the last few years, many banks have acquired an Internet presence, with a Web site and facilities for customers to manage their accounts online.*
- They also issue credit cards that customers use to shop online, and they acquire the resulting transactions from merchants.
- To protect this business, they use standard Internet security technology:
  - **SSL/TLS encryption** built into Web browsers, and
  - **Firewalls** to prevent people who hack the Web server from tunneling back into the main bookkeeping systems that lie behind it.

Banking Computer Security

- Banking computer security is important for a number of reasons.
- Until quite recently, banks were the main **nonmilitary market** for many computer security products, so they had a disproportionate influence on **security standards**.
- Second, even where their technology isn't blessed by an international standard, it is often widely used in other sectors anyway.
- Burglar alarms originally developed for bank vaults are used everywhere from jewelers' shops to the home;
  - they are even used by supermarkets to detect when freezer cabinets have been sabotaged by shop staff who hope to be given the food that would otherwise spoil. ☺

Air Force Base

- *Some of the most sophisticated installations are the **electronic warfare systems** whose goals include trying to block enemy radars while preventing the enemy from blocking yours.*
- This area of **information warfare** is particularly instructive because for decades, well-funded research labs have been developing sophisticated countermeasures, counter-countermeasures, and so on—with a depth, subtlety, and range of deception strategies that are still not found elsewhere.
- Their use in battle has given insights that are not available anywhere else.
  - These insights are likely to be valuable now that the service-denial attacks, which are the mainstay of electronic warfare, are starting to be seen on the Net, and now that governments are starting to talk of "**information warfare.**"

Air Force Base

- ***Military communication systems*** *have some interesting requirements.*

- It is often not sufficient just to **encipher messages**:
  - an enemy, who sees traffic encrypted with somebody else's keys may simply locate the transmitter and attack it.

- **Low-probability-of-intercept** (LPI) radio links are one answer;
  - they use a number of tricks, such as **spread-spectrum modulation**, that are now being adopted in applications such as copyright marking.

Air Force Base

- *Military organizations have some of the biggest systems for logistics and inventory management, and they have a number of special assurance requirements.*
- For example, one may have a separate stores management system at each different security level:
  - a general system for things like jet fuel and boot polish, plus a second secret system for stores and equipment whose location might give away tactical intentions.
    - (This is very like the business that keeps separate sets of books for its partners and for the tax man)
- There may also be **intelligence systems** and **command systems** with even higher protection requirements.
  - The general rule is that sensitive information may not flow down to less-restrictive classifications.

Nuclear Weapons

- *The particular problems of protecting **nuclear weapons** have given rise over the last two generations to a lot of interesting security technology.*
- These range from:
  - **electronic authentication systems**, which prevent weapons being used without the permission of the **national command authority**,
  - **seals** and **alarm systems**,
  - methods of identifying people with a high degree of certainty using **biometrics** such as **iris patterns**.

Hospital Security

- *As Web-based technologies are adopted in hospitals, they present interesting new assurance problems.*
- For example, as reference books—such as directories of drugs—are moved online, doctors need assurance that **life-critical data** (such as the figures for dosage per body weight) are exactly as published by the relevant authority, and have not been mangled in some way, whether accidental or deliberate.
- Many of these safety problems could affect other Web systems in a few years' time.
- Another example is that as doctors start to access Web pages containing **patients' records** from home or from laptops in their cars,
  - suitable electronic **authentication** and **encryption** tools are starting to be required.

Hospital Security

- *Patient record systems should not let all the staff see every patient's record, or privacy violations can be expected.*
- These systems need to implement rules such as, "nurses can see the records of any patient who has been cared for in their department at any time during the previous 90 days."
  - This can be hard to do with traditional computer security mechanisms, as **roles can change** (nurses move from one department to another).
  - And there are **cross-system dependencies** (the patient records system may end up relying on the personnel system for access control decisions).
- Applications such as these are inspiring research in **role-based access control**.

Hospital Security

- *Patient records are often **anonymized** for use in research, but this is difficult to do well.*
- Simply **encrypting patient names** is usually not adequate, as an enquiry such as "Show me all records of 59-year-old males who were treated for a broken collarbone on September 15, 1966," would usually be enough to find the record of a politician who was known to have sustained such an injury as a college athlete.
- But if records cannot be anonymized properly, then much **stricter rules** will usually have to be followed when handling the data, and this will increase the cost of medical research.

Hospital Security

- *New technology can introduce risks that are just not understood.*
- Hospital administrators understand the need for **backup procedures** to deal with outages of power, telephone service, and so on, but medical practice is rapidly coming to **depend on the Net** in ways that are often not documented.
- For example, individual clinical departments may start using:
  - **online drug databases**;
  - stop keeping adequate paper copies of **drug formularies**
  - **never inform** the contingency planning team.
- So **attacks that degrade network services** (such as viruses and distributed denial-of-service attacks) might have serious consequences for medical practice.

Home Security

- *Many people use some of the systems we've already described.*
- You may use a Web-based electronic banking system to pay bills; and
  - in a few years you may have encrypted online access to your medical records.
- Your burglar alarm may send an encrypted "all's well" signal to the security company every few minutes,
  - rather than waking up the neighborhood when something happens.
- Your car may have an **electronic immobilizer** that sends an **encrypted challenge** to a radio transponder in the key fob;
  - the transponder has to respond correctly before the car will start.
  - since all but the most sophisticated thieves now have to take the car away and fit a new engine controller before they can sell it, this makes theft harder, and reduces your insurance premiums.
- However, it also increases the number of car-jackings: criminals who want a getaway car are more likely to take one at gunpoint.

Home Security

- *Early mobile phones were easy for villains to "clone."*
- Users could suddenly find their bills inflated by hundreds or even thousands of dollars.
- The current GSM digital mobile phones authenticate themselves to the network by a cryptographic **challenge-response protocol** similar to the ones used in car-locks and immobilizers.

Home Security

- Satellite TV set-top boxes **decipher movies** as long as you keep paying your subscription;
- DVD players use copy control mechanisms based on **cryptography** and **copyright marking** to make it harder to copy disks (or to play them outside a certain geographic area).
- In many countries, households that can't get credit can get **prepayment meters** for electricity and gas, which they fill using a smartcard or other electronic key which they refill at a local store.
- Many **universities** use similar technologies to get students pay for photocopier use, washing machines, and even soft drinks.

Security: a bright future ☺

- The chances are that you already use many systems that enforce some protection policy or other using largely electronic mechanisms. Over the next few decades, the number of such systems is going to increase rapidly.
  - **Unfortunately, based on past experience, many of them will be badly designed. The necessary skills are just not spread widely enough.**
- The aim of this book is to **enable you to design** such systems better.
  - To do this, an engineer or programmer needs to learn about current systems, how they work, and—at least as important—how they have failed in the past.
- Civil engineers learn far more from the one bridge that falls down than from the hundred that stay up;
  - **exactly the same holds in security engineering.**

How large is the field?

Applied cryptography and network security

- Stallings, *Cryptography and Network Security: Principles and Practice, 4/e* (Prentice Hall, 2006). The network security components and an extra chapter on SNMP are also packaged as Stallings' *Network Security Essentials: Applications and Standards, 3/e* (Prentice Hall, 2007).
- Kaufman, Perlman and Speciner, *Network Security: Private Communications in a Public World, second edition* (Prentice Hall, 2003).
- Menezes, Van Oorschot and Vanstone, *Handbook of Applied Cryptography* (CRC Press, 1996; 2001 with corrections), free online for personal use.

How large is the field?

Computer and operating system security

- Stallings and Brown, *Computer Security: Principles and Practice* (Prentice Hall, 2007).
- Gollmann, *Computer Security, 2/e* (Wiley, 2006).
- Bishop, *Computer Security: Art and Science* (Addison-Wesley, 2002). Shorter version which "omits much of the mathematical formalism": *Introduction to Computer Security* (Addison-Wesley, 2005).
- Pfleeger and Pfleeger, *Security in Computing, 4/e* (Prentice Hall, 2007).

How large is the field?

Software security

- Viega and McGraw, *Building Secure Software* (Addison-Wesley, 2001).
- Howard and LeBlanc, *Writing Secure Code, second edition* (Microsoft Press, 2002).

How large is the field?

Mobile code security, malicious code and web security

- McGraw and Felton, *Securing Java: Getting Down to Business with Mobile Code* (Wiley, 1999; 1st edition: Java Security, 1997), free online web edition.
- Stein, Web Security: A Step-By-Step Reference Guide (Addison-Wesley, 1998).
- Rubin, Geer and Ranum, *Web Security Sourcebook: A Complete Guide to Web Security Threats and Solutions* (Wiley, 1997).
- Rubin, White-Hat Security Arsenal (Addison-Wesley, 2001).

How large is the field?

Firewalls and more

- Cheswick and Bellovin, *Firewalls and Internet Security*, *first edition* (Addison-Wesley, 1994); free online for personal use. Second edition with Rubin (Feb. 2003).

How large is the field?

Security infrastructures and digital signatures

- Adams and Lloyd, *Understanding Public-Key Infrastructure, second edition* (Macmillan Technical, 2002).
- Housley and Polk, *Planning for PKI: Best Practices Guide for Deploying Public Key Infrastructures* (Wiley, 2001).

How large is the field?

Security in the real-life systems

- Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems, 2/e* (Wiley, 2008). The first edition (2001) is available free online.
- Schneier, *Secrets and Lies: Digital Security in a Networked World* (Wiley, 2000).

Definitions: System

- The first thing we need to clarify is what we mean by ***system***. In practice, this can denote:
  1. A product or component, such as a cryptographic protocol, a smartcard, or the hardware of a PC.
  2. A collection of the above plus an operating system, communications, and other things that make up an organization's infrastructure.
  3. The above plus one or more applications (accounts, payroll, design and so on).
  4. Any or all of the above plus IT staff.
  5. Any or all of the above plus internal users and management.
  6. Any or all of the above plus customers and other external users.
  7. Any or all of the above plus the surrounding environment including the media, competitors, regulators, and politicians.

Definitions: Principal

- In the literature on security and cryptology, it's a convention that **principals in security protocols** are identified by names chosen with (usually) successive initial letters—much like hurricanes—and so we see lots of statements such as, "Alice authenticates herself to Bob."
- This makes things much more readable, but often at the expense of precision.
  - Do we mean that Alice proves to Bob that her name actually is Alice, or that she proves she's got a particular credential?
  - Do we mean that the authentication is done by Alice the human being, or by a smartcard or software tool acting as Alice's agent?
- In that case, are we sure it's Alice, and not perhaps Cherie to whom Alice lent her card, or David who stole her card, or Eve who hacked her PC?

Definitions: Principal

- By a **subject** we mean a physical person (human, ET, . . .), in any role including that of an operator, principal, or victim.
- By a **person**, we mean either a physical person or a legal person such as a company or government.

Definitions: Principal

- A **principal** is an entity that participates in a security system.
  - This entity can be a subject, a person, a role, or a piece of equipment, such as a PC, smartcard, or card-reader terminal.
- A principal can also be a **communications channel** (which might be a port number or a crypto key, depending on the circumstance).
- A principal can also be a **compound of other principals**; examples are a group (Alice or Bob), a **conjunction** (Alice and Bob acting together), a **compound role** (Alice acting as Bob's manager), and a **delegation** (Bob acting for Alice in her absence).

Definitions: Principal

- **Beware that groups and roles are not the same**.
- By a **group** *we* mean a set of principals, while a **role** is a function assumed by different persons in succession (such as "the officer of the watch on the USS Nimitz" or "the president for the time being of the Icelandic Medical Association").
- A principal may be considered at more than one **level of abstraction**;
  - for example, "Bob acting for Alice in her absence" might mean "Bob's smartcard representing Bob who is acting for Alice in her absence" or even "Bob operating Alice's smartcard in her absence."
- When we have to consider more detail, we'll be more specific. ☺

Definitions: Identity

- The meaning of the word **identity** is controversial.
- We will use it to mean a correspondence between the names of two principals signifying that they refer to the same person or equipment.
  - For example, it may be important to know that the Bob in "Alice acting as Bob's manager" is the same as the Bob in "Bob acting as Charlie's manager" and in "Bob as branch manager signing a bank draft jointly with David."
- Often, the term identity is abused to mean simply "name," an abuse entrenched by such phrases as "user identity" and "citizen's identity card."

Definitions: trust and trustworthy

- The definitions of **trust** and **trustworthy** are often confused.
- The difference:
  - if an NSA employee is observed in a toilet stall at Baltimore Washington International Airport selling key material to a Chinese diplomat, then (assuming his operation was not authorized) he can be described as "**trusted but not trustworthy**."
- Hereafter, Iwe'll use the NSA definition that a **trusted** system or component is one whose failure can break the security policy, while a **trustworthy** system or component is one that won't fail.

Definitions: trust

- Beware, though, that there are **many alternative definitions** of trust.
- A U.K. military view stresses **auditability** and **fail-secure** properties:
  - a trusted systems element is one “whose integrity cannot be assured by external observation of its behavior while in operation.”
- Other definitions often have to do with whether a particular system is **approved by authority**:
  - a trusted system might be “a system that won’t get me fired if it gets hacked on my watch” or even “a system that we can insure.”
  - We won’t use either of these definitions. When we mean a system that isn’t failure-evident, or an approved system, or an insured system, we’ll say so.

Definitions: Confidentiality

- The definition of **confidentiality** versus **privacy** versus **secrecy**.
- These terms clearly overlap; but, equally clearly, they are not exactly the same.
- If my neighbor cuts down some ivy at our common fence with the result that his kids can look into my garden and tease my dogs, **it's not my confidentiality** that has been invaded.
- And the duty to keep quiet about the affairs of a former employer is a duty of **confidence**, not of privacy.

Definitions: Confidentiality, privacy, secrecy.

- **Secrecy** is a **technical term** that refers to the effect of the mechanisms used to limit the number of principals who can access information, such as cryptography or computer access controls.
- **Confidentiality** involves an obligation to protect some other person's or organization's secrets if you know them.
- **Privacy** is the ability and/or right to protect your personal secrets;
  - It extends to the ability and/or right to prevent invasions of your personal space (the exact definition varies quite sharply from one country to another).
  - Privacy can extend to families but not to legal persons such as corporations.

Definitions: Privacy

- Thus, for example, hospital patients have a **right to privacy**; in order to uphold this right, the doctors, nurses, and other staff have a duty of confidence toward their patients.
- The hospital has no right of privacy in respect of its business dealings, but those employees who are privy to them may have a duty of confidence.
- **So, in short, privacy is secrecy for the benefit of the individual, while confidentiality is secrecy for the benefit of the organization.**

Definitions: Anonymity

- There is a further complexity in that it's often **not sufficient** to keep the contents of messages secret.
  - For example, many countries have laws making the treatment of sexually transmitted diseases secret, yet a private eye who could find out that you were exchanging encrypted messages with an STD clinic might well draw the conclusion that you were being treated there.
- So one may also have to **protect metadata** such as the source or destination of messages.
- **Anonymity** can be just as important a factor in privacy (or confidentiality) as secrecy.
  - To make things even more complex, some writers refer to what we've called secrecy as ***message content confidentiality***, and to what we've called anonymity as ***message source (or destination) confidentiality***.

Definitions: Authenticity and integrity

- The meanings of **authenticity** and **integrity** can also vary subtly.
  - In the academic literature on security protocols, **authenticity means integrity plus freshness**: you have established that you are speaking to a genuine principal, not a replay of previous messages.
- There is a similar idea in **banking protocols:**
  - In a country whose banking laws state that checks are no longer valid after six months, a seven-month-old uncashed check **has integrity** (assuming it has not been altered), **but is no longer valid**. (Bankers would not use the word *authenticity* in this context.).
- **The military usage** of **authenticity** tends to apply to the identity of principals and orders they give, while **integrity** applies to stored data.

Definitions: Vulnerability

- A **vulnerability** is a property of a system or its environment, which, in conjunction with an internal or external **threat**, can lead to a **security failure**, which is a state of affairs contrary to the system's security policy.

- By **security policy** we mean a clear statement of a system's protection strategy
  - For example, "each credit must be matched by an equal and opposite debit, and all transactions over $1,000 must be authorized by two managers".

Definitions: Security Target

- A **security target** is a more detailed specification, which sets out the means by which a security policy will be implemented in a particular product:
  - encryption
  - digital signature mechanisms,
  - access controls,
  - audit logs,
  - and so on

and which will be used as the yardstick to evaluate whether the designers and implementers have done a proper job.

- Between these two levels we may find a **protection profile**, which is like a security target except written in a sufficiently **device independent way** to allow comparative evaluations among different products and different versions of the same product.

It is impossible to foresee the consequences of being clever.

CHRISTOPHER STRACHEY

Passwords

- Only amateurs attack machines, professionals target people.

Bruce Schneier

Humans and Passwords

- ***Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations. (They are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed. But they are sufficiently pervasive that we must design our protocols around their limitations.)***

KAUFMAN, PERLMAN, AND SPECINER

Human Computer Interaction

- Taking care of old-fashioned **access control tokens** such as metal keys is a matter of common sense.
  - But common sense is **not always adequate** for the measures used to protect computer systems.

- The human-machine gap causes security problems in a number of contexts, from straightforward system administration to the ways in which users **mismanage** security products such as **encryption software**.

- However, most of the problems arise in a simple context in which they are relatively easy to analyze and discuss—

The management of passwords.

Other passwords

- In addition to things that are “obviously” passwords, such as the password you use to log on to your computer and the PIN that activates your bank card, there are **many other things** (and **combinations of things**) that have an equivalent effect.

- The most notorious are the **Social Security numbers** and your mother’s maiden name, which many organizations use to recognize you.

- For example, AT&T’s wireless service contract states that anyone who knows your name, address, phone number and the last four digits of your social security number is authorized to make changes to your account. ☺

Identity Theft

- The ease with which such personal data can be guessed or found out from more or less public sources has given rise to a huge **identity theft** industry.
- Criminals obtain credit cards, mobile phones, and other assets in your name, use them, and leave you to sort out the mess.
- In the United States, about **half a million** people are the victims of this kind of fraud each year.

Passwords

- Passwords are one of the biggest practical problems facing **security engineers** today.
  - They are the foundation on which much of **information security** is built.
- Remembering a password is **contingent on frequent use** (so that passwords are imprinted well on memory) and **consistent context** (so that different passwords do not interfere with each other in memory).
  - Neither of these conditions is met when people are asked to choose passwords for a large number of Web sites that they visit rarely.
- So as they become principals in more and more electronic systems, the **same passwords get used over and over again**.
  - Not only may attacks be carried out by outsiders guessing passwords, but by insiders in other systems.

Authenticating people

- In a typical system, human users must authenticate themselves to a client (which may be a PC, a mobile phone, an ATM, or whatever), and the client in turn authenticates itself to one or more servers or services (such as an electronic banking system or a phone company).

- **Authenticating electronic devices to each other is a more or less manageable problem (at least in theory).**

- **Authenticating people to devices is more difficult.**

Authenticating people to devices

There are basically three ways:

1. The first is that the person retains **physical control** of the device—as with a remote car-door key, a PDA, or even a laptop computer.
2. The second is that he or she presents **something he or she knows**, such as a password.
3. The third is to use a **biometric**, such as a **fingerprint** or **iris pattern**. (These options are commonly summed up as "something you have, something you know, or something you are.")

- **For reasons of cost, most systems take the second option**.
  - Even where we use a physical token such as a hand-held password generator, it is common to use a password as well to lock it.

Passwords Matter

- Passwords matter, and managing them is a serious real-world problem.

- We'll look at the **human issues** first, then at the different kinds of **attack model**, and finally at technical **attacks** and **defenses**.

- All of these issues are important, so tackling only one of them is likely to lead to a bad design.

Applied Psychology Issues

There are basically three types of concern:

1. Will the user break the system security by **disclosing the password to a third party**, whether accidentally, on purpose, or as a result of deception?

2. Will the user **enter the password correctly** with a high enough probability?

3. Will users **remember the password**, or will they have to either write it down or choose one that's easy for the attacker to guess?

Social Engineering

- One of the most **severe practical threats** to the confidentiality of information is that the attacker will extract it directly, from people who are authorized to access it, by telling some **plausible untruth**.
- This attack, known as **social engineering**, deals with medical systems, as it is the main current threat to medical privacy.
  - The typical perpetrator is an insurance investigator who phones a hospital or doctor's office pretending to be a doctor involved in the emergency care of the target of investigation.
- This technique, also known as '**blagging**' in Britain and '**pretexting**' in America, is widely used to extract information from banks, insurance companies, and other firms that hold personal information;
  - Some people earn a living at it. ☺

False pretext calls

- Passwords are often extracted by **false pretext phone calls**. A harassed system administrator is called once or twice on trivial matters by someone who claims to be a very senior manager's personal assistant; once he has accepted the caller's story, she calls and urgently demands a **high-level password** on some plausible pretext.
- Unless an organization has well-thought-out policies, attacks of this kind are very likely to work.
- In a **systematic experimental study**, for example, 336 computer science students at the **University of Sydney** were sent an email message asking them to supply their password on the pretext that it was required to "validate" the password database after a suspected break-in.
  - 138 of them returned a valid password. Some were suspicious: 30 returned a plausible-looking but invalid password, while over 200 changed their passwords without official prompting.
- **But very few of them reported the email to authority.**

Controlling False Calls

- One company controls this vulnerability with a policy that states:
  - *"The root password for each machine:*
    - *shall be too long to remember, at least 16 alpha and numeric characters chosen at random by the system;*
    - *shall be written on a piece of paper and kept in an envelope in the room where the machine is located;*
    - *may never be divulged over the telephone or used over the network;*
    - *may only be entered at the console of the machine that it controls."*
- If a rule like this is rigidly enforced throughout an organization, a pretext attack on a root password becomes conspicuous, and is much less likely to succeed.

Controlling False Calls

- Another approach, used at the NSA, is to have **different-colored** internal and external **telephones** that are not connected to each other, and rules that when the **external phone in a room is off-hook**, classified material can't even be discussed in the room, let alone on the phone.

- A somewhat less extreme approach (used at Cambridge laboratory) is to have **different ring tones** for internal and external calls.
  - This works as long as you have alert system administrators.

- **Physical authentication devices**, like the password generators, are even better but are often too expensive, incompatible with legacy systems, or contrary to some policy (whether reasonable or not).

Reliable Password Entry

- The second human issue is that if a password is **too long** or complex, the user might have **difficulty entering** it correctly.
  - A long random password may confuse the person entering it, and if the operation they are trying to perform is **urgent**, this might have **safety** or **other implications**.
- One application in which this is important is **encrypted access codes**.
  - By quoting a reservation number, we get access to a hotel room or rental car. Airline ticketing is going this way, with many operators giving passengers a number to quote at the departure gate rather than a boarding card.
- As the numbers get longer, what happens to the error rate?

Reliable Password Entry

- An interesting study was done in South Africa, in the context of the prepaid electricity meters used to sell electricity in areas where the customers have no credit rating and often not even an address.
- With one make of meter, the customer hands some money to a sales agent, and in return gets one or more **20-digit numbers** printed out on a receipt.
- He takes this receipt home and enters the numbers at a keypad in his meter.
- These numbers are **encrypted commands**, whether to dispense electricity, to change the tariff or whatever; the meter decrypts them and acts on them.

Reliable Password Entry

- When the meter was introduced, there was concern that since about a third of the population was illiterate, and people might get lost halfway through entering the number, this meter might be unusable in practice.

- But it turned out that **illiteracy was not a problem**; even people who could not read had no difficulty with numbers ("Everybody can use a phone," as one of the engineers said).

- **Entry errors** were a greater problem, but were solved by printing the 20 digits in two rows, containing, respectively, three and two groups of four digits.

Firing codes ☺

- A quite different application is the firing codes for U.S. nuclear weapons.
- These consist of **only 12 decimal digits**.
- If they are ever used, it is likely that the operators will be under the **most extreme stress**, and possibly using improvised or obsolete communications channels.
- Experiments suggested that 12 digits was the maximum that could be **conveyed reliably** in such circumstances.

Remembering Passwords

- The greatest source of complaints about passwords is the fact that most people **find them hard to remember**.

- Twelve to twenty digits may be fine when they can be simply copied from a telegram or a meter ticket, but when customers are expected to memorize passwords, they either:
  - choose values that are **easy for attackers to guess**, or
  - write them down or
  - Both ☺

Remembering Passwords

- The problems are not limited to computer access.
- For example, one chain of hotels in France introduced completely **unattended service**.
  - You would turn up at the hotel, swipe your credit card in the reception machine, and get a receipt with a numerical access code that would unlock your room door.
  - To keep costs down, the rooms did not have en suite bathrooms, so guests had to use communal facilities.
  - The usual failure mode was that a guest, having gone to the bathroom, would **forget his access code.**
  - Unless he had taken the receipt with him, he'd end up having to sleep on the bathroom floor until the staff arrived the following morning.
- Problems related to password memorability can be discussed under two main headings:
  - **design errors**, and **operational failures**.

Design Errors

- Attempts to design systems so as to make passwords memorable are a frequent source of severe design errors—especially with the many systems being built rapidly by **unskilled people for electronic business**.
  - An instructive, and important, example of **how not to do it** is to ask customers for "**your mother's maiden name**."
- Many banks, government departments, and other organizations authenticate their customers in this way.
- There are two rather obvious problems:
  - First, your mother's maiden name **is easy for a thief to find out**, whether by asking around, chasing birth and marriage records, or using online genealogical databases.
  - Second, even if you decide that from now on your mother's maiden name is going to be, say, Yngstrom (or even yGt5r4ad), rather than Smith, there are problems.
    - You might break your credit card agreement, and perhaps invalidate your insurance cover, by **giving false data**.

Design Errors

- Moreover, asking for a maiden name makes assumptions that don't hold for all cultures
  - Icelanders have no surnames, and women from many other countries don't change their names on marriage.
- There might be no provision for changing such a password, so if it ever becomes known to a thief you could have to close and reopen bank accounts.
- Finally, you will be asked to give it to a lot of organizations, any one of which might have a crooked employee.
  - You could always tell "Yngstrom" to your bank. "Jones" to the phone company, "Geraghty" to the travel agent, and so on; but data are **shared extensively between companies**, so you could easily end up confusing their systems (not to mention yourself).

Design Errors

- Slightly more thoughtfully designed e-commerce sites **ask for a password explicitly** rather than a maiden name.
  - But the sheer number of applications for which the average person is asked to use a password nowadays exceeds the powers of human memory.
- So either customers will **write passwords down** (**despite being told not to**) or they will **use the same password** for many different purposes.
  - Thus, the password you use to authenticate the customer of the electronic banking system you've just designed, is quite possibly known to a Mafia-operated porn site as well. ☺

Design Errors

- The risk you face as a consumer is not just a direct loss through **identity theft** or **fraud**.

- **Badly designed password mechanisms** can undermine your credibility and can cause you to lose a genuine legal claim.
  - For example, if a thief manages to forge a copy of your cash machine card, then steals your bank account, the bank will ask whether you have ever shared your personal identification number with any other person or company.
- If you admit to using the same number for your mobile phone, the bank may well say that either you were grossly negligent by allowing someone to see you using the phone, or somebody at the phone company must be to blame.
  - **In either case, it's up to you to find them and sue them**.

Design Errors

- Some organizations try to find other security information.
- One bank asks its business customers **the value of the last check** from their account that was cleared.
- In theory, this could be a good system: it has the advantage that even if someone compromises my password—such as by overhearing me doing a transaction on the telephone—the security of the system usually recovers more or less automatically.
- The implementation details bear some attention though.
  - You wonder whether a supplier, to whom you'd just written a check, had a chance of **impersonating you**.
- **Conclusion: asking for the last three checks' values would be safer.**
  - But the problem might be different. Having given the checkbook to our accountant for the annual audit, we could not authenticate ourselves to get a balance over the phone and we have to visit the branch.

Design Errors: PIN

- Attempts to find alternative solutions have more often hit the rocks.
- One bank sent its customers a letter warning them against writing down their PIN, and instead supplied a distinctive piece of cardboard on which they were supposed to conceal their PIN in the following way: suppose your PIN is 2256.
- Choose a four-letter word, say blue. Write these four letters down in the second, second, fifth, and sixth columns of the card, respectively, as shown in Figure.
- Then fill up the empty boxes with random letters.

1	2	3	4	5	6	7	8	9	0
	b								
	l								
				u					
					e				

Figure 3.1 A bad mnemonic system for bank PINs.

Design Errors: PIN

- This is clearly a bad idea. Even if the random letters aren't written in a slightly different way, a quick check shows that a 4 by 10 matrix of random letters may yield about two dozen words (unless there's an "s" on the bottom row, when you can get 40 to 50).

1	2	3	4	5	6	7	8	9	0
	b								
	l								
				u					
					e				

Figure 3.1 A bad mnemonic system for bank PINs.

Design Errors: PIN

- Some banks allow customers to **choose their own PINs**.
  - It is believed that about a third of customers use a **birthdate**, in which case the chances against the thief are now a bit over 100 to 1 (and much shorter if the thief knows the victim).
- Even if this risk is thought acceptable, the PIN might still be set to the **same value as the PIN used with a mobile phone** that's shared with family members.
- To analyze this problem, we have to consider a number of different **threat models**.

Operational Issues: Shock ☺

- A failure to think through the sort of rules that organizations should make, and enforce, to support the password mechanisms they have implemented has led to some **really spectacular cases**.
- One important case in Britain in the late 1980s was *R v. Gold and Schifreen*.
- The defendants saw a phone number for the development system for Prestel (an early public email service run by British Telecom) in a note **stuck on a terminal at an exhibition**.
  - They dialed in later, and found that the welcome screen had an all powerful maintenance password displayed on it. They tried this on the live system, too, and it worked!
  - They proceeded to take over the Duke of Edinburgh's electronic mail account, and sent mail 'from' him to someone they didn't like, announcing the award of a knighthood.
- This crime so **shocked** the establishment that when prosecutors failed to convict the defendants under the laws then in force, Parliament passed Britain's first computer crime law.