Implementing Cryptography #2

Ed Zaluska

COMP6230:

Implementing Cybersecurity

Data Encryption Standard (DES)

- 1977, mandatory for US Government agencies (for non-secret communication)
- major influence on modern cryptography – hence an important case study - but also *still in use* today (see later)
- IBM design (from earlier work on *Lucifier*)
- **block cipher**: 64-bit block, 56-bit key
- original lifetime ten years – reviewed in 1983, 1987, 1993 (3DES/TDES introduced)

DES (2)

- finally replaced by AES in 2002
  (Advanced Encryption Standard)
- US Government agencies required to switch to AES, but DES still perfectly acceptable for many ‘legacy’ applications and also high-value bank transfers (3DES)
- Note that the **algorithm was published**
- P = 64 bits, K = 56 bits, C = 64 bits

Kerckhoff's principle

(Flemish military cryptographer, 1883)

- "A cryptosystem must be secure even if everything about the system (apart from the key) is public knowledge"

  (Exact *opposite* of 'security by obscurity')
- the entire cryptographic community worldwide has been trying to break DES for the last 35 years: very little success

DES (3)

- “Why a published security standard – shouldn’t it be ‘top secret’?”
- many examples of ‘secret’ systems that were broken despite the secrecy

  (Japanese “Purple” cipher in WW II just one well-known example)
- DES now not considered secure – why?
- the main problem is the key length (56 bits), which is now considered too short

  (N.B. IBM designed DES to be hard to implement in software, to discourage supercomputer attack: software implementations use a lot of look-up tables!)

‘Brute Force’ Attack

- assume a ‘known plaintext’ attack (i.e. the P/T and the resulting C/T are both known)
- the key can ***always*** be recovered by an exhaustive search of the entire key space

  000000000000000…….0

  000000000000000…….1 etc

  up to

  111111111111111…….1
- DES has 2**56 possible keys (7 10**16)

DES ‘Cracker’

- a DES ‘cracker’ (to search the entire key space) was proposed in 1977 ($20M)
- a cracker was finally built in 1998 by the ‘Electronic Frontier Foundation’ (www.eff.org) at a cost of $250k – won a $10k prize for the ‘DES Challenge II’ in less than 3 days.
- financial institutions still use Triple DES (3DES/TDES), which *remains* effectively unbreakable (hence secure)
- focus of security attacks shifts to *obtaining keys*

How long to test DES key space?

- 56 bits requires 2**56 (or 72 10**15) tests
- (for entire space: key will be found on average after testing half the keys)
- assume 1 million test every second (guess)
- 31 10**6 seconds in a year, hence an exhaustive search would require 2000 years.
- EFF DES cracker tests 43,000 in parallel
- a key length of 56 bits was long enough in 1977, but not with modern hardware…

DES no longer secure…

- the limited 56-bit key length is the reason DES had to be replaced by AES: the minimum AES key size is 128 bits
- still no real algorithmic weakness known in DES after more than 30 years study…
- the DES design principles were originally classified – some suspicion at the time because the NSA were known to have advised on the design…

Differential cryptanalysis

- Controversy about NSA involvement in DES design since 1977 – was there a secret ‘back door’ built into DES so that the NSA could read enciphered messages? (see Crypto AG case)
- 1990 Biham and Shami invented a new crypto attack (differential cryptography) and published a paper on their new technique
- the method attempts to discover non-random behaviour by changing the input and exploiting this to recover the key – successful against many ciphers in common use, but not DES!
- DES designed to protect against such attacks!
- Both IBM and NSA knew about the technique in 1974 (but kept it secret)

Double DES?

- increase effective key length with a double encryption? (i.e. encrypt with K1, then encrypt resulting C/T with K2)
- unfortunately, the combined system does not have an effective key length of 112, but only 57
- *‘meet in the middle’* attack: store all possible intermediate ciphertexts from first key, then decrypt C/T with second key and look for a match.

“meet-in-the-middle attack”

- “known plaintext attack” assumption
- assume P encrypted with K1 gives INT1i
  (“INT” = intermediate result)
- compute all of these (i.e. for all K1) and store them (you will need a lot of memory!)
- now decrypt C with K2 for all K2: this produces a series of INT2i results
- as each INT2i is generated, search for a corresponding INT1i result: if found, success!
- So the worst-case time is 2**56 + 2**56 encrypts

Triple DES

- 3DES (or T-DES)
- either use 3 different 56-bit keys
  (effective key size 112 bits)
- or use 2 different 56-bit keys K1 and K2,
  (encrypt K1, decrypt K2, encrypt K1)
  (set K1 = K2, equivalent to legacy single-DES)
  (effective key size about 80 bits)
- secure and currently widely-used for financial transactions (ok up to about 2029?)