Encryption 3
Tom Chothia
Computer Security: Lecture 4

This Lecture
• Some more history (not on the exam)
• RSA
• Signing
• Pretty Good Privacy, PGP

Some History
Before cheap powerful computers, unbreakable encryption was almost impossible.
Governments wanted to read the codes of others.
They could control the export of these machines.
When IBM designed DES they could get it weakened.

Some History
During 1970-1990 all that changed.
Personal computers could do anything a cipher machine could do.
University academics worked on encryption with the aim of making it available to everyone.

RSA
• RSA is the most popular public key cipher.
  – It uses two large primes p & q.
    We set n = p.q and \( o(n) = (p-1)(q-1) \)
  – Pick random
  – The public key is (e,n) and the private key is (d,n)

RSA
• To encrypt a message, turn it into numbers “m” that are less than “n”
  • The encrypt as cipher text c do:
    \( c = m^e \mod n \)
• To decrypt a cipher text c as a message m do:
  \( m = c^d \mod n \)
Elliptic curve crypto

- Public key encryption based on elliptic curves.
- Functionally very like RSA, but more efficient.
- No full security proof, but recommended by NSA.
- Becoming the most popular web public key encryption system.

Using Public Key Crypto

- Public key crypto is much slower than symmetric key.
- So instead of just using public key crypto, systems:
  - make a new symmetric key
  - encrypt that with the public key
  - then encrypt the message with the symmetric key.

Some More History

- These ciphers make encryption pretty much unbreakable.
- They made encryption available to everyone and the Internet, as we know it, possible.
- But Diffie, Rivest, etc. weren't the first. At the British intelligence service GCHQ:
  - James Ellis invented the concept of public keys in the 1960s
  - Malcolm J. Williamson invented DH in 1974
  - Clifford Cocks invented RSA in 1973
- But GCHQ distributed their keys via embassies, so never used it.

Signatures

- Using RSA $E_{pub}(D_{priv}(M)) = M$
- This can be used to sign messages.
- Sign a message with the private key and this can be verified with the public key.
- Any real crypto suite will not use the same key for encryption and signing.
  - as this can be used to trick people into decrypting.

Signatures

Alice has a and a signing key $K_s$ and wants to sign message $M$

Signature:

$D_{ks}(\#(M))$  \hspace{2cm} \text{Plain Text}$

RSA decrypt with key $ks$

SHA hash

Clear-signed: $M,D_{ks}(\#(M))$

Pretty Good Privacy

- In 1991 Phil Zimmermann implemented RSA in an e-mail friendly package.
- He wanted encryption for everyone, especially activists.
- RSA inc. started a licensing dispute.
- The US government started a criminal investigation for arms trafficking!
The Crypto Wars

- Laws in the 1990s were unable to cope with strong encryption from short computer programs.
- Strong crypto available for free on the new Internet panic governments.
- Who was going to control crypto in the age of the Internet?

Key Escrow

- Early 90’s government barging:
  - You can use Strong Crypto, but you have to give us the key.
- Implemented in “Clipper Chip”
  - Strong crypto
  - Every message includes with a Law Enforcement Access Field (LEAF) which contains the key
  - LEAF encrypted with a key the government knows.

Matt Blaze’s Analysis of Clipper Chip

- Clipper chip must test the integrity of the LEAF and only accept connections if it is genuine.
- Matt Blaze found that this was based on a 16 bit checksum in the LEAF.
  - 16 bits can be brute force, so LEAFs can be forged.
- I.e you could use the clipper check without real key escrow

SkipJack

- The Clipper chip used the NSA designed cipher SkipJack:
  - 80 bit key, unlike DES’s 56 bit key.
- As soon as it was declassification Biham and Shamir found a weakness.
- Today it can be broken in $2^{44}+2^{16}$ ops
  - About the same as DES.

First Set Paper:

Key Escrow from a Safe Distance
Looking Back at the Clipper Chip
By Matt Blaze

27th Computer Security Applications Conference, ACSAC 2011. Find a link to it on the module website.
The Crypto Wars

  – Due partly to Matt Blaze’s analysis
  – and strongly attack by John Kerry among others.

• 2000 US laws lifted: the Geeks ”won the crypto wars”.

• Freedoms won in the US then filtered through to the rest of the Internet,
  – e.g. French laws until 2004: ECB mode only, max key length 40, must include known plain text.

Crypto Wars: Round 2

• We learnt in September that the NSA had been working to weaken (”back door”) crypto.

• Some of the possible backdoors:
  – “Bad” elliptic curve parameters
  – Weak random number generators: e.g. Dual_EC_DRBG

Certificates

• A public key certificate binds a public key to an identity.

• As well as a public key it contains a name, e-mail address, etc.

• It is signed, with the private key, and anyone else that trusts it.

Distributing Public Keys

• The whole system breaks down if you get the wrong key for someone.

• If someone you trust has signed some else key you can may trust it too.

Key Servers

• Key servers store public key certificates

• Many clients can automatically search a key server for unknown e-mail addresses.
  – But beware, there is no gautenete the key is not a fake.

https://xkcd.com/364/
Recommended Key Lengths

- See http://www.keylength.com/

This Lecture

- Some more history (not on the exam)
- RSA
- Signing
- Pretty Good Privacy, PGP

Further Reading

- See links on the website.
- Eike’s Cryptology module
- Coursera Cryptology module
  - www.coursera.org/course/crypto
- Bruce Schneier: Applied Cryptography

Next Lecture

- Access Control Frameworks