Selected Topics

Computer Security Lecture 16

Mike Just[1]

School of Informatics
University of Edinburgh

11th March 2010

[1] Based on original lecture notes by David Aspinall

Outline

Introduction

Hidden Communications

Anonymous Communications

The Dining Cryptographers

Zero-knowledge protocols

Secret Sharing

Introduction

- Cryptography and computer security can be applied in many weird and wonderful ways to solve many problems
- Sometimes the problems are isolated or impractical
- But sometimes they relate to very practical, real problems
- The reality though is that today, many of these solutions have not yet been widely adopted - users and developers seem to have enough trouble with hashes, certificates and digital signatures
- Remember: For many of today's IT problems, solutions that deal with the people and processes would be sufficient (though are difficult to realize)
- The technical solutions remain viable, and can still contribute to these and other problems, in some cases negating the need for people and process solutions

Hidden Communications

- Steganography has a long history, from ancient use of hidden inks to cold-war era use of microdots. Many cryptographic techniques exist to hide information inside any kind of data files, including text, images, sound files, or movies.
- You can **hide data in noise** present in media files, e.g., using least-significant bits of PNG files or WAV files. (Lossy compression is harder: need techniques which take into account the compression method).
- You can **hide data as other data**, for example, using controlled-random generation from natural language grammars, or more generally but less controllably, by compressing data and then running media-specific compression algorithms *in reverse* to fabricate images or sounds.

Hidden Communications . . .

- You can use **secret sharing** to spread information around, e.g., several GIF images on web must be combined to reveal.
- Similar techniques are used for *watermarking* and *fingerprinting* for **content protection**.
- Disadvantage of steganography is that it fails Kerchoff's principle, by relying on secret methods: **security through obscurity**.
- Once methods are discovered, it may be possible to "sanitize" files to remove stega, or at the least, to corrupt it (e.g., removing mp3 stega messages apparently isn't possible without significant loss of quality (why? – because of re-encoding).
- Can combine with encryption, but that requires key sharing

Dear Friend , We know you are interested in receiving cutting-edge news ! This is a one time mailing there is no need to request removal if you won't want any more . This mail is being sent in compliance with Senate bill 1916 ; Title 3 ; Section 303 ! This is a ligitimate business proposal . Why work for somebody else when you can become rich inside 96 weeks . Have you ever noticed nearly every commercial on television has a .com on in it and how long the line-ups are at bank machines . Well, now is your chance to capitalize on this . We will help you process your orders within seconds and use credit cards on your website . You can begin at absolutely no cost to you ! But don't believe us . Prof Anderson of Nebraska tried us and says "I was skeptical but it worked for me" . We are a BBB member in good standing . We implore you - act now ! Sign up a friend and you'll get a discount of 20offer . Dear Business person ; This letter was specially selected to be sent to you . If you are not interested in our publications and wish to be removed from our lists, simply do NOT respond and ignore this mail ! This mail is being sent in compliance with Senate bill 1619 , Title 6 ; Section 308 ! This is not multi-level marketing ! Why work for somebody else when you can become rich within 44 MONTHS . Have you ever noticed more people than ever are surfing the web plus society seems to be moving faster and faster . Well, now is your chance to capitalize on this ! WE will help YOU sell more and SELL MORE . You can begin at absolutely no cost to you . But don't believe us ! Mrs Anderson who resides in Alaska tried us and says "Now I'm rich, Rich, RICH" ! We assure you that we operate within all applicable laws ! We beseech you - act now ! Sign up a friend and you'll get a discount of 10Bless .

This slide is not real spam but *spam mimic*, hiding a 22 character message.

Covert channels in signature schemes

- Apart from the (risky) possibility of hiding information in plaintext messages, covert (aka "subliminal") channels exist in some signature schemes themselves, including DSA.
- General protocol:
  1. Alice, a prison inmate, writes an innocuous message
  2. Using a secret key she shares with Bob, she signs the message in such a way as to hide a message in the signature.
  3. She sends the signed message to Bob. As a matter of routine, it is intercepted by the prison warden who checks the contents is innocuous, and that the signature verifies.
  4. Bob receives the package, ignores the innocuous message, and retrieves the hidden communication using the shared key.
- To prevent this possibility, **subliminal-free signature schemes** have been developed.

Anonymous Communications

- Basic idea: **anonymous remailer** accepts incoming email, strips origin headers, replaces with anonymised addresses before forwarding on to destination. Remailer keeps password-protected anonymous accounts.
- Variations: web-based remailers; anonymous Usenet posting; using PGP signatures for pseudonyms. Anonymising web proxies.
- Security risks: tracking; flooding/replay to determine destination; forged mail. Also **law enforcement** to force revelation of identities.

Anonymous Communications . . .

- Security enhancements: remailer public-key encryption for condidentiality; randomised padding, latency and re-ordering to help defeat traffic analysis; **chaining** several remailers (chain as strong as *strongest* link); secret splitting and broadcasting.
- Many uses, immoral (e.g., criminal: drug dealing, money laundering), moral (e.g., counselling, whistle-blowing), and frivolous. Anonymity already a basic component in society (gossip; government; press).

The Dining Cryptographers

- How can we broadcast a secret message so everyone can read it, but no one knows where it comes from? Anonymous posters/remailers are imperfect since Internet messages can be traced, at least in principle.
- David Chaum described the *dinining cryptographers* problem: three cryptographers are eating dinner. Waiter tells them the bill has been settled, but won't say who by: it may be one of them or may be the NSA. Cryptographers have a dilemma: they respect need for anonymity, but don't want to accept any gratuities from the NSA.

The Dining Cryptographers . . .

- Solution (1-bit communication): each crypto'r flips coin, shows person on his right the result. Each crypto'r announces whether two coins he sees are same/different. If one wants to communicate he paid for meal, he flips the result. Result is 1 if number of differences is odd.
- No. of adjacent diffs in coins is 0 or 2. If one person communicates, number will be 1 or 3. This system has **unconditional security** if no collusion occurs.
- Based on "Dining Philosophers" problem, where n philosophers sit around a table with n chopsticks, so one is between each pair. Must have agreement on scheduling in order to avoid deadlock.
- DC works because no. of pairwise differences should be zero or two.
- Each philosopher sees two coins, and cannot know the third or who is sending the message.

Zero-knowledge protocols

- A problem with traditional password-style authentication schemes is that to to prove you know a secret, you are forced to reveal the secret.
- With **zero-knowledge protocols**, Peggy can prove (to a high degree of certainty) to Victor that she knows something, without giving Victor any knowledge beyond that fact — even the possibility to prove the fact to a third party. (Peggy is the "prover", Victor is the "verifier").

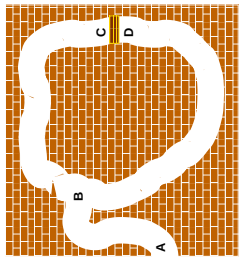
Zero-knowledge protocols . . .

- A basic ingredient for zero-knowledge protocols is **cut and choose**, the classic protocol for dividing anything fairly. For example, to prevent Peggy and Victor squabbling over the size of a cake portion:
  1. Peggy cuts the cake in half
  2. Victor chooses one of the halves for himself
  3. Peggy takes the other half.

  It's in Peggy's best interests to divide as fairly as she can in the first step, because Victor will choose whichever half looks larger in the second step!

The zero-knowledge cave

Peggy knows the magic words to open a secret door and wants to prove this to Victor without giving the words away.



1. Victor waits at A while Peggy runs past B either way, to the door.
2. Victor goes to point B. He can't see Peggy.
3. Victor shouts for Peggy to come out of the right- or left-hand passage.
4. Peggy comes out the way that Victor asked, opening the magic door if necessary.
5. They repeat until Victor is convinced Peggy knows the magic words.

Zero-knowledge protocols, cont'd

- After n iterations, probability of Peggy fooling Victor is $\frac{1}{2^n}$.
- Basic real protocol has following outline. Assume that Peggy has some secret information p and that this is the solution to a hard problem P.
  1. Peggy uses p and a random number r to transform P into an isomorphic hard problem P'.
  2. She solves this problem using p and r, and commits to the solution with a bit-commitment scheme.
  3. Peggy tells Victor P'. (This gives him no information about p.)
  4. Victor asks Peggy either to
     - prove that $P \simeq P'$, or
     - open the solution she committed to and prove it solves P'.
  5. Peggy complies. They repeat n times.
- Possible hard problems include NP-complete probs or RSA problem (used in **Guillou-Quisquater** protocol). Many non-trivial ZK variations, including *non-interactive* and *parallel* versions.

Blind signatures

- Sometimes we want documents to be signed without the signer knowing their contents, or not knowing their exact contents.
- **Completely blind signatures**: Alice takes her message M and multiplies it by some random **blinding factor** R. She asks Bob to sign RM, and then divides out the blinding factor to leave the original document signed by Bob. (This exact method only works for schemes where multiplication and signing are commutative).
- For RSA, to blind sign message m, A computes random $1 \leq r \leq n-1$ where $gcd(r, n) = 1$ and sends $c = mr^e \bmod n$ to B for signing.
- B computes $s' = c^d \bmod n = m^d r \bmod n$ and returns to A.
- A computes the signature $s = s'r^{-1} \bmod n = m^d \bmod n$

Secret sharing

- Many high-security applications require participation from more than one user.
- One obvious scheme may be to use **repeated encryption**: give n people n keys K_i, and encrypt a message with each key in turn:

  $$\{\{\cdots\{M\}_{K_1}\cdots\}_{K_{n-1}}\}_{K_n}$$

  But this is not necessarily a good strategy.
- A more secure and simpler method is **secret splitting** by inventing $n-1$ random nos $M_1 \cdots M_{n-1}$ and setting $M_n = R - (M_1 + \cdots + M_{n-1})$. (Addition might be bitwise XOR, or addition modulo).
- More complicated **threshold schemes** allow reconstruction with m-out-of-n shares. One technique is to use a point in m-dimensional space, and each share is an $m-1$-dimensional hyperplane, randomly chosen to intersect with the point.