There won't be a revision lecture for the Computer Security module. Instead, these notes are provided to help you prepare for the exam.

Revision advice

- Focus on understanding principles, not learning boring details. You don't need to be able to recall a lot of detail that you would normally access in books or on the web. However, you do need to demonstrate thorough understanding. In exams that I set, if lot of detail is needed to answer a question, that detail will be given as part of the question.

  Example:
  - You don't need to know the details of the FOO'92 protocol. An exam question that asks about FOO'92 would remind you of the details. However, you need to demonstrate thorough understanding. (Exam question 3, 2009.)
  - Similarly, you don't need to remember all the details of the attestation protocol from trusted computing, but you have to demonstrate understanding of it (Exam question 3, 2008).

- Working on past exam questions is a good idea. Past questions are available on the module web page. But please bear in mind that the set of topics covered in each year varies considerably. Only topics of this year will be in this year's exam. They are marked with * on the module page.

Exam advice

- Answer the question posed (and only the question posed). Try to make your answer as simple as possible, while ensuring it fully answers the question. You won't get credit for saying things that are not asked for in the question.
  - DO: Read the question fully. Don't guess what it says.
  - DO: If the question asks for a yes/no answer, be sure you say "yes" or "no", unambiguously.
  - DO: If the question asks you to "give your reasons" or "explain your answer", give the reasons or the explanation.
  - DON'T: Don't write random facts that you think are vaguely related to the question. It is just wasting your time.
  - DON'T: Write hurriedly, or change your mind while writing. It will result in an answer that is not intelligible, and you will get 0.
  - DON'T: Write a long essay. A short answer that directly addresses the question is worth much more than a long waffly one, and will be marked accordingly.

- Your answer must be absolutely clear, totally legible, and precise and concise.
Getting advice from me

Instead of attending a revision lecture, you are invited to ask me questions by email during Revision Week 1 (26-30 April 2010). I will send my replies to the entire set of students on the module (but I will remove your name, so people won't know who asked what question).

I will provide model answers for up to three exam questions. To vote on which ones you would like, use this doodle poll. You must vote by 30 April 2010.

http://www.doodle.com/p75mnpa3qx8qypfn

Past exam question

Here, we look at a past exam question, and some answers that were submitted. Try yourself to mark the answers, before looking at the marks they actually got.

The question...

3. Key certificates

(a) What is a certificate authority? Explain a scenario in which they are useful. [9%]

(b) What is the web of trust model in PGP? [8%]

(c) Alice receives an email, apparently signed using a PGP private key by Bob. She does not know Bob's public key, but she knows and has signed the public keys of Carol and Dave. Dave has signed the keys of Alice, Bob and Eve. Eve has signed Carol's and Dave's keys. Alice has "complete trust" in Dave, and "part trust" in Carol and Eve. Should Alice accept the signature on Bob's email? Explain your answer, specifying any assumptions you make about PGP. [8%]

(d) Sally has gone to the police with an email she says is from Richard, in which he threatens to kill her. Richard denies writing the email, even though it is signed with his PGP key, and plenty of Richard's friends have digitally signed Richard's key certificate confirming that it is indeed his PGP key. The police consult you in order to find out whether it can be proved beyond reasonable doubt that Richard wrote the email. Advise them. [8%]

The answers...

We look at some answers to part (a) only.
3. (a) If A has complete trust in B, and B has complete trust in C, then when A signs B’s public key, B signs C’s public key, A can sign C’s public key without knowing C. This is certificate authority.

Because in this way we don’t need a big computer to remember every body’s public key. We can save the cost and increase the communicating speed.

Remarks:

• The examiner will spend 3 seconds to come to the conclusion that this answer is nonsense. The examiner will not try to make sense of it or find parts of it that have a snippet of truth. He will simply give it zero.

• Note that it doesn't say what a CA is, and it doesn't give anything like what one could call a scenario in which CAs are useful.

Mark awarded: 0/9
A certificate authority (CA) is one who assures that A's public key is A's and not anybody else's. The CA can do this by signing A's public key with his private key.

A scenario where B does not trust CA but trusts B can be sure that A's public key is A's because it is being ensured by CA.

\[ B \xrightarrow{\text{trusts}} CA \xrightarrow{\text{trusted}} A \xrightarrow{\text{signed}} A. \]

Thus, B trusts A.

Remarks

- It does not make sense to say "assures that A's public key is A's". It is necessarily the case that what belongs to A belongs to A. However, the definition is basically correct.
- The example scenario is nonsense. Firstly, it is not a scenario in which a CA is useful; it is rather an elaboration of how the writer thinks a CA is used. Secondly, it seems to want to conclude that a CA helps an agent B to trust an agent A. This is incorrect. A CA merely testifies to A's public key; it does not help you decide whether to trust A or not.

Marks awarded: 3/9.
Answer 3

B. Key certificates

(a) Certificate authority is an assertion that a certain key belongs to a certain entity, which is signed by another entity.

For example, if you want to browse a web page of Yahoo, your browser need to verify the web site is secure. The web site will send a certificate signed by a third-trusted party to verify it is good. If your browser has trusted the third-trusted party, it will trust the web site. We call it trust chain.

Remarks

- A certificate authority is not an assertion.
- "Your browser needs to verify that the web site is secure" -- too vague. What exactly does it verify, and how? "If you want...", "your browser..." -- it is better to use professional language rather than colloquial language.
- The scenario isn't properly detailed. What is the exact security guarantee? Trust in the target web site (yahoo above) is not the issue.

Mark awarded: 3/9
Answer 4

Remarks

- Since the word "authority" is part of what we are trying to define, we should avoid using it in the definition. "Ensure" is an inappropriate word here. A CA testifies, asserts, or signs, or states; but it doesn't ensure.
- The scenario given seems to have the right idea about the possibility that someone might be pretending to be someone else, but it suggests that the CA can directly assure that information comes from an entity, which is incorrect.
- The answer doesn't mention public keys, which are a crucial aspect of certificate authorities.

Mark awarded: 5/9. That was probably too generous.
Answer 5

3. a) A certificate authority is an entity that provides signed documents which certify that a certain key belongs to a certain entity. The certificate authority signs these documents with its private key and usually is well-known and trusted. A scenario where certificate authorities are useful is the following: Alice wants to send a message to Bob encrypted with his public key. She is not sure how to obtain it in order to be sure that it is his key and not somebody else's. If Bob has a certificate signed by a certificate authority, he can provide it along with the key to convince her.

Remarks

- A good answer. The definition and the scenario are clear.
- One might quibble about the word "document".

Mark awarded: 9/9.
A certificate authority is an entity that issues public key certificates -- that is, digitally signed statements asserting that a certain key is the public key of a certain entity.

- A certificate authority is useful if one entity A wishes to reliably ascertain the public key of another, B, say in order to send B a message encrypted with its public key. The entity A can obtain B's public key certificate from a certificate authority that it trusts.
- A certificate authority is useful if, for example, a user A wishes to obtain a secure web session with her bank B. A's browser software can obtain B's public key certificate from a certificate authority, and thereby be sure that the session really is with B and not with an imposter.

Remarks:
- The question is of the form "What is X?". Therefore the answer should begin "X is...". It is quite difficult to construct a good sentence that begins "A certificate authority is...", but that is what is required.
The two bullet points are alternatives. I would award full marks to the first paragraph plus either of the bullet points.

(b) What is the web of trust model in PGP? [8%]

The web of trust model is a mechanism for confirming that a certain entity owns a certain public key. It works by adding up degrees of trust from several other entities. The evidence that entity Alice has that entity Bob's public key is a certain value is computed by adding up the evidence she has about the public key of each person who has signed key certificates linking Bob to that key.

Remarks:

- Again, a "what is X?" question, so the answer must begin "X is...". You probably cannot say exactly what it is in a single sentence, though, so you can add more sentences. Make sure each of your additional sentences contributes directly to explaining what it is.

(c) Alice receives an email, apparently signed using a PGP private key by Bob. She does not know Bob's public key, but she knows and has signed the public keys of Carol and Dave. Dave has signed the keys of Alice, Bob and Eve. Eve has signed Carol's and Dave's keys. Alice has "complete trust" in Dave, and "part trust" in Carol and Eve. Should Alice accept the signature on Bob's email? Explain your answer, specifying any assumptions you make about PGP. [8%]

Yes, Alice should accept the signature, assuming that the signature is valid. She trusts Dave completely and knows his key. Dave has signed Bob's key, so according to the rules of PGP, Alice should accept the value for Bob's key. She can use it to verify the signature on his email. If the signature is valid using Bob's public key, then she should accept it.

Remarks:

- The question demands a yes/no answer, so you should almost always begin "Yes" or "No". In this case, the question didn't say whether the signature is valid, so we can add that proviso.
- If a question demands a yes/no answer but there are circumstances that you need to take into account that are not defined in the question, you could explain those rather than give a direct "yes"/"no".

(d) Sally has gone to the police with an email she says is from Richard, in which he threatens to kill her. Richard denies writing the email, even though it is signed with his PGP key, and plenty of Richard's friends have digitally signed Richard's key certificate confirming that it is indeed his PGP key. The police consult you in order to find out whether it can be proved beyond reasonable doubt that Richard wrote the email. Advise them. [8%]

Whether this evidence is sufficient or not depends on some circumstances which are not specified in the question -- e.g., whether other people could have sent the email on behalf of Richard, by using his computer while he is logged in but temporarily absent, by obtaining his private key from a disk, by coercion, etc. The police should be advised to investigate these possibilities. It is also possible that the public key is not Richard's, even though other people have signed saying it is. The police should also consider that possibility.