THE UNIVERSITY OF AUCKLAND

SECOND SEMESTER, 2004
Campus: City

COMPUTER SCIENCE

Software Security

(Time Allowed: TWO hours)

NOTE: Attempt **ALL** questions in the 12-page script book provided. Total possible: **100 marks**.

CONTINUED

1. Consider the following security objective from "A Security Analysis of SERVE".

> SERVE attempts to separate the name of the voter from his/her vote through the use of public key cryptography...

Summarise this objective in a single English word (*e.g.* "integrity"); then very briefly explain why your summary is appropriate, in approximately 25 words. **[5 marks]**

2. Consider the following technological description of SERVE:

> ... In each voting district that is participating in SERVE, a local election official (called the LEO by SERVE) generates ... a key pair. The LEO's public key is used to encrypt (scramble) the ballots of SERVE voters from that district. Once a ballot has been encrypted, it can be read only if it is decrypted through the use of the unique private key known only to the LEO.
>
> When the voter uses SERVE to cast a ballot, his/her web browser sends the completed ballot, along with identifying information such as the voter's name, to a SERVE web server. This information is transmitted to SERVE in encrypted form, sent in a way that only the SERVE web server can decrypt it. Because the ballot is encrypted before transmission, if someone were to intercept the encrypted ballot en route, it would be impossible to decipher the actual vote. Note that, at this point, the LEO's key pair has not yet been used.
>
> When the ballot is received, SERVE verifies that the voter is registered and has not yet voted. SERVE decrypts the ballot using the SERVE private key, separates the ballot from the voter's name, and then encrypts the ballot (without the voter's name) using the LEO's public key. Therefore, only the appropriate LEO will be able to decrypt the encrypted ballot. The encrypted ballot is stored for later transmission to the LEO. SERVE retains the encrypted ballot, even after a copy has been sent to the LEO. SERVE also places the voter's name on a list of people who have already cast a vote, so that they will not be allowed to vote a second time.

Classify this defensive strategy using Lampson's taxonomy: isolate, exclude, restrict, recover, punish. Justify your classification, in approximately 25 words. **[5 marks]**

3. Consider the following security analysis of the SERVE architecture:

> ... the LEO could deduce how voters in his/her precinct have voted by downloading votes from SERVE so frequently that they get at most one new vote and voter name each time. Recall that the LEO can request from SERVE a list of names of voters from the LEO's district who have already voted via the Internet and the list (re-ordered randomly) of encrypted ballots for those voters. If a curious LEO makes the request sufficiently often, it should be possible to infer how each individual voter voted, an obvious ... risk.

Illustrate this threat using the "abuse frame" notation. For full credit, your diagram must have descriptive labels for the vulnerabily (or vulnerabilities), the asset(s) under attack, the agent(s), the antirequirement(s), and the phenomena (edges) linking these entities. **[15 marks]**

4. Name a defensive strategy (using Lampson's taxonomy) that could be used to lessen the threat of question 3, and briefly describe a technological implementation of this strategy, using approximately 50 words. **[10 marks]**

5. In "Single Sign-On Architectures", the operation of a Public Key Infrastructure-based (PKI-based) SSO architecture is described in the following passage.

> … users first register themselves at a trusted authentication authority (in this case called a certification authority (CA)) or at one of the authentication authority's registration agents (called registration authorities (RAs)). During this registration process different things occur: users identify themselves using a set of credentials; a piece of client-side software generates an asymmetric key pair; and the public key of this key pair is offered to the CA (or RA) for certification. Upon receipt of the user's credentials and the public key, the CA (or RA) will verify the user's credentials. If the credentials are valid it will generate a public key certificate and send it back to the user. The user's public key certificate and the user's private key are cached on the user's machine (or on a smart card or cryptographic token). They both are used to generate a kind of software tokens similar to the ones used in token-based SSO systems. These tokens are used to prove the user's identity to other secondary authentication authorities in subsequent authentication requests.

In the case of a PKI-based SSO with a single CA and no RA, what are the security implications when the CA is unavailable? Your answer should be approximately 75 words, and should discuss confidentiality, integrity, and availability. **[15 marks]**

6. Consider the following passage, quoted from Peter Gutmann's "Simplifying Public Key Management".

> … existing protocols originally designed to rely on a global PKI must either employ ad hoc solutions or use any public key that turns up, because the only alternative is not to use any keys at all. In the absence of a PKI, system administrators can incorporate alternative approaches [such as key continuity] …

Critically and appreciatively discuss Gutmann's comments, quoted above, in the context of the SSO architecture described in question 5 above. Your discussion should be approximately 75 words in length. For full credit you should consider the functions required of a PKI by SERVE, and the possible use of key continuity as a replacement for one or more of these functions. **[15 marks]**

7. Is the Georgia Tech Honeynet an example of an intrusion detection system? Justify your answer briefly, in approximately 50 words, using appropriate definitions and terminology from your required readings. **[10 marks]**

8. Judge David Harvey, in his presentation to our class entitled "Recent Developments in Copyright", pointed out that transient copying is technologically required when viewing copyright works in digital form. However any unauthorised copying is an infringement of the reproduction right of copyright owners in New Zealand, unless the unauthorised copying is a permitted use. Briefly describe two different ways that New Zealand copyright law could be amended, to allow legal viewing of copyright digital works in New Zealand. Your answer should be approximately 25 words. **[5 marks]**

9. Markus Kuhn has pointed out that it is possible for an eavesdropper to detect, at a distance, what is being displayed on someone else's flat-panel display. Consider this detection process from an ethical and legal perspective, in the New Zealand context. Discuss the legal and ethical constraints on the eavesdropper. For full credit, your discussion must use terminology and concepts from your required readings (including the lecture slides). Your answer should be approximately 50 words. **[10 marks]**

CONTINUED

10. Several of the required readings in this class described security systems that rely on "black boxes" to hold secrets or compute functions. Briefly describe the functions and implementations of two of these black boxes from your readings, using approximately 25 words to describe each black box. **[10 marks]**