Our exam has been postponed till Thursday, which makes much more sense than having an exam and then one more class before Spring Break. So now you get one more chance for questions.

I have yet to receive a project proposal, although I have had some discussions with one of you. The syllabus is the syllabus, and a ‘0’ on a component of the grade worth 30% will not have a pleasant effect on your final grade.

Authentication

While waiting for the exam to begin let us look ahead to some of the issues we will talk about after Spring Break. Most of them are concerned with some kind of authentication, rather than mere cryptology. This became a viable issue after the revolution caused by the invention of public key cryptography, although there are uses for private key cryptography in these applications. The topics include

- Digital Signatures: a secure way to verify that a document has been "signed" electronically, in a way that your confidence that the signature was not forged is equivalent to a handwritten signature

- Message Authentication, that is, some kind of digital proof that a received message (stock trade order, military orders, ...) is authentic, rather than a spoof. This is different from digital signatures because it allows the possibility that more than one agent can send an authentic message.

- email and internet security

We will also be discussing detection of intruders and their malware, as well as firewalls.

Authentication

There are many aspects of message authentication. Stallings lists eight possible attacks that might be aided or thwarted by proper authentication protocols.

1. Disclosure: keep someone else from reading the message, at least for a while. This is pure cryptography.

2. Traffic Analysis: in the evenings before the US invasion of Panama to remove Manuel Noriega from power, there were an unusually large number of takeout pizza orders from the Pentagon.
3. **Masquerade:** Messages from a fraudulent source that pretend to be from someone genuine. This would include false military orders ("Delay the attack!"), dirty tricks (e.g., a false email from a politician to a known criminal), or other fraud. This is pure authentication.

4. **Content Modification:** Various changes to content of messages, including the insertion of a trojan horse or other malware into software or other document with executable macros.

5. **Sequence Modification:** Change of sequence of messages. This might be used in stock market fraud, for example, changing the order of sell and buy requests..

6. **Timing Modifications:** Hold a message until a more appropriate time, or replay a message from earlier. One example of this was a fraudulent scheme at a racetrack in Québec in the 1970s. After the race was over, the computer running the track’s wagering system was halted manually, a winning ticket was quickly printed, a fraudulent bet was entered into memory (add one to the number of legitimate winning tickets), and then the computer was restarted. This was easy on the PDP-11 if you had physical access to the machine and knew the memory locations of the binary (no virtual memory). The timing involved was almost too quick to be noticed by a human observer.

7. **Source repudiation:** "That’s not my signature."

8. **Destination repudiation:** "We never got that email."

---

**Techniques**

The major symmetric authentication technique is a Message Authentication Code, or MAC. This depends on the message $M$ and a shared key $K$. Alice sends message $M$ to Bob and includes the MAC from $K$ and $M$. Bob gets the message (in the clear) and uses $K$ to recompute the MAC. If he gets the one that Alice sent, then he begins to believe that the message $M$ is authentic.

The MAC needs to be short but secure: the MAC algorithm being an implementation of a one-way function. Otherwise, an eavesdropper can derive $K$ from the MAC.

A MAC is not a digital signature, since more than one person has the key.