

## Review #1

List of topics covered in class:

1. Privacy/Cryptography
2. Identity theft/Authentication
3. Intrusion
4. Denial-of-service
5. Viruses
6. Worms
7. Honeypots
8. Privacy/Anonymization
9. IP spoofing
10. Infrastructure attacks
11. Social engineering

### **Group A**

You have a goal to protect communications between an online bank and its clients. The bank stores client account information on a database server. Clients can access this server *from any machine in the Internet* and perform transactions or view the balance. Bank must protect the privacy of transactions and must assure that no one can forge transactions. It is not imperative that bank service be available at all times, although extended periods of non-operation would hurt the profits. It is very important that transaction data is never lost.

- a) List all possible threats that this bank should protect from. Use the list of topics covered in class as a reference.
- b) Suggest how you would protect against the threats listed in a). For each solution you propose give sufficient implementation details (e.g. if you use cryptography specify whether it is symmetric or asymmetric, and suggest an example encryption protocol) and elaborate why you have chosen this approach. Do not forget to specify how you would organize administration support for the solution you propose, i.e. how much human intervention is needed.
- c) Discuss expected performance and cost of your solution (just in terms good/bad and large/small).

### **Group B**

You have a goal to protect military communications. You will only protect communications between wired machines and you can obtain a list of machines belonging to the military. These machines are scattered all over the world and belong to different networks, but they are under central administration. Users are expected to log on locally to one of the machines and then communicate with the other machines in the regional network (e.g. other machines within military network in Germany). Occasionally, users need to communicate with a machine in a military network that is

outside their region (e.g. from a machine in Germany to a machine in US). Users may also access Internet freely. Mail service is the only service on the military network that is available 'from the outside'; i.e. users can log on to a military mail server within their regional network to check their E-mail *from any machine in the Internet*. Military network must protect the privacy of all communication and must assure that no one can forge communications. It is imperative that all services be available at all times. It is also important that no data is lost from the machines.

- a) List all possible threats that this network should protect from. Use the list of topics covered in class as a reference.
- b) Suggest how you would protect against the threats listed in a). For each solution you propose give sufficient implementation details (e.g. if you use cryptography specify whether it is symmetric or asymmetric, and suggest an example encryption protocol) and elaborate why you have chosen this approach. Do not forget to specify how you would organize administration support for the solution you propose, i.e. how much human intervention is needed.
- c) Discuss expected performance and cost of your solution (just in terms good/bad and large/small).

### **Group C**

You have a goal to secure the University of Delaware network. This network is used by students and staff for research purposes. It offers several public services: DNS, mail and Web service. Those services can be accessed by clients *from any machine in the Internet*. Network should make a reasonable attempt to protect the privacy of its communications and must assure that no one can forge those communications that are sensitive (e.g., post a fake grade). It is not imperative that network services be available at all times, although extended periods of non-operation should be avoided. It is very important that important data (e.g. student records) is never lost. The University network is large and consists of many machines with different operating systems scattered in labs. There are also student laptops that can be connected to the University network and become a part of it at any time. The University has scarce financial resources dedicated to network security.

- a) List all possible threats that this network should protect from. Use the list of topics covered in class as a reference.
- b) Suggest how you would protect against the threats listed in a). For each solution you propose give sufficient implementation details (e.g. if you use cryptography specify whether it is symmetric or asymmetric, and suggest an example encryption protocol) and elaborate why you have chosen this approach. Do not forget to specify how you would organize administration support for the solution you propose, i.e. how much human intervention is needed.
- c) Discuss expected performance and cost of your solution (just in terms good/bad and large/small).

### **Group D**

- a) Imagine that you are a worm writer. Your goal is to write such a worm that infects a very large number of machines, in spite of installed defenses. You don't care if this happens within a day or a year, but you want as a large number of machines as you can get. When all machines have been infected you would like each one of them to commence a DDoS attack on the target you select at that time. Describe how you would write this worm. What characteristics it would have?
- b) Now discuss what approach could be taken *by a single network* to defend against the worm you proposed in a). Assume that worm code is not known at the time defenses are designed. If it seems that no complete solution is possible discuss if there is anything that can at least improve the situation. For each approach you propose discuss expected performance and cost (just in terms good/bad and large/small). Network's first priority is not to be infected at all, its second priority is to stop worm from propagating further and the third priority is to avoid participation in the DDoS attack.
- c) Now discuss what approach could be taken *by the whole Internet community* to defend against the worm you proposed in a). Assume that worm code is not known at the time defenses are designed. If it seems that no complete solution is possible discuss if there is anything that can at least improve the situation. For each approach you propose discuss expected performance and cost (just in terms good/bad and large/small). Internet's first priority is to limit the number of infected machines, its second priority is to prevent/defend from the DDoS attack.