

SI110 Introduction to Cyber Security
Technical Foundations

Name: _____

Alpha: _____

Hand in a stapled, printed copy with your answers.

Homework: /SI110/Cyber Operations/Case Studies

A. First, read these articles:

<http://www.informationweek.com/news/government/security/229700151>
<http://www.informationweek.com/news/security/attacks/229400810>
<http://arstechnica.com/security/news/2011/06/rsa-finally-comes-clean-secrid-is-compromised.ars>
<http://www.wired.com/threatlevel/2011/08/how-rsa-got-hacked/>

B. After you have read the articles, answer these questions:

1. RSA was compromised using "spear-phishing" that targeted a "zero-day".
 - a. Define phishing.
 - b. Define zero-day.
 - c. Describe the spear-phishing email:
 - (1) From whom did it appear to have been sent?
 - (2) What was the subject line?
 - (3) To whom was it sent?
 - (4) What was attached?
 - d. Concerning the zero day:
 - (1) It exploited what software?
 - (2) The exploit installed a variant of what?
 - e. Concerning the installed exploit:
 - (1) What type of malware is it?
Go to the below URL, search for the exploit you named in 1.d.(2)
http://www.f-secure.com/en/web/labs_global/threats/descriptions
 - (2) From information on that page, answer these questions:
 - Is it always installed in the same location in the filesystem?
 - Does it always have the same file size?
 - Is it started when the infected computer boots?
 - Can it bypass firewalls?
 - In your opinion, what is the most dangerous of it's "operations" and why?
 - (3) What information was first gained by the attacker?
 - (4) How was this information then used?
 - (5) What was done at the "staging servers" ?
 - (6) What occurred in the Conclusion phase of the attack?
 - (7) Where was the data sent?
2. Describe how SecurID works.
3. On what two things did the security of SecurID ultimately rest?

C. Hand in this sheet, stapled as a coversheet to a typed, printed copy of your answers.