CS55N: Ten Ideas in Computer Security **Fall 2005**

Course Project

Due: Tuesday, Dec. 6th, 2005.

- Choose only **one** of the following projects.
- You are expected to use the web for your research.
- You may work in pairs for any of the programming projects.

Writing projects

Control Hijacking Attacks. Write a report describing at least five recent ideas in mounting control hijacking attacks. Propose a single mechanism that can prevent all such attacks. Try to think of attacks that will defeat your mechanism.

Here are a few potential starting points:

- `http://research.microsoft.com/users/jpincus/beyond-stack-smashing.pdf`
- `http://www.phrack.org/phrack/56/p56-0x0e`
- `http://www.securityfocus.com/archive/1/7480`

Web Site Security. Write a report describing at least five ideas in exploiting web site weaknesses. Propose a single mechanism that can prevent all such attacks. Try to think of attacks that will defeat your mechanism. Here are a few potential starting points:

- `http://www.packetstormsecurity.org/papers/general/whitepaper_httpresponse.pdf`
- `http://www.cert.org/archive/pdf/cross_site_scripting.pdf`
- `http://www.securiteam.com/securityreviews/5TP0F0UEVQ.html`
- `http://www.nextgenss.com/papers/advanced_sql_injection.pdf`

Entropy of common identifiers. Your goal is to determine how difficult it is to guess someone's social security number or creditcard number, assuming you know a little about the person.

- **Social Security Numbers:**
  - What is the total number of issued social security numbers (SSNs)?
  - Suppose you know a person's date of birth; what is the total number of SSNs you would need to search through?
  - Suppose you know both the person's date of birth and where they applied for an SSN; what is the total number of SSNs you would need to search through?
  - What other information will help you guess a person's SSN?

To get started, take a look at:
`http://privacy.cs.cmu.edu/dataprivacy/projects/ssnwatch/`

- **Credit Card Numbers:**
  - What is the format of a creditcard number? What do the different digits mean?
  - What information is stored on the magnetic strip?
  - How large is the set of valid creditcard numbers that can be issued?
  - Suppose you know what bank issued a person's creditcard, what is the total number of creditcard numbers you would need to search through?
  - What other information will help you guess a person's creditcard number?

Programming projects

Anonymizer. Your goal is to implement a simple web anonymizer. Your code will run on your machine and accept SSL connections from browsers around the around. It will forward the requests to the target web site and relay the response back to the browser issuing the request. Since the user wishes to remain anonymous from the web site, your goal is to properly scrub cookies set by the site.

Browser history privacy violations. Write a web page containing Javascript that finds the list of slashdot articles previously read by someone visiting your page. Your Javascript should obtain a list of current links on slashdot and then display to the user a subset of links he visited. The user visiting your site will see the contents of your site along with a list of slashdot articles he recently read.

History privacy violation vulnerability:
`http://seclists.org/lists/bugtraq/2002/Feb/0271.html`