**ITEC 345: Course paper/report.**

**Due 2013.May.09 (Thu) 17:00 sharp, on D2L dropbox**

You need to pick a topic to research and write a report (3-5 pages long) on that topic. I have provided a few sample topics below. If however, you have any other topic in mind, please let me know. The report must closely adhere to the format of an IEEE research paper, including citations. A sample format in MS word is [available](http://www.radford.edu/itec345/2013spring-ibarland/Homeworks/paper/paper-format-sample.docx). Your paper’s bibliography[[1]](#footnote-1) does *not* contribute toward the page count. Be sure your paper is well-written; you (or a lucky roommate) should give it a close read just before submitting, to catch any grammatical errors, missing words, inconsistent verb tenses, and the like.

In all cases, giving specific details and concrete examples and techniques is more important than giving general-but-nonspecific overviews. For example, rather than:

* “Email is insecure, because messages can be forged.”

Instead, explain how:

* “Email using SMTP doesn’t require authentication: it can be forged. The SMTP server receiving a message simply receives a string stating who the message is purportedly from; anybody connecting to the SMTP server can provide any message and claim any originator.” Even better, demonstrate your point, perhaps including an appendix with a sample SMTP exchange, with the sender’s text in green, and the SMTP server’s output in black:

220 rucs.radford.edu ESMTP Postfix (Ubuntu)

MAIL FROM:imposter@doppelganger.com

250 2.1.0 Ok

RCPT TO:victim@gmail.com

250 2.1.0 Ok

DATA

354 End data with <CR><LF>.<CR><LF>

subject: help

As a Nigerian prince, I demand your bank account number!

.

250 2.0.0 Ok

The first version doesn’t necessarily demonstrate any understanding, while the second version explains and *specifically* demonstrates why.

Similarly: Rather than just say loosely “DES is insecure”, be more precise: “An attacker can break DES with a brute-force attack: the 56-bit key has 256 ~ 72 quadrillion possible values. Although this is very large, it is on the edge of feasible: a network of 1000 students, using off-the-shelf desktop computers (3GHz processors), each taking 100 cycles to do each the 16-rounds of DES, could crack any key within 1.2yrs.”

If you find yourself using terms like “can hack into” and “highly insecure”, strive to give concrete examples instead.

**Possible Topics** (with some *possible* resources)**:**

- Survey the security of Web-browser extensions

* + - Resources**:**
			1. <http://webblaze.cs.berkeley.edu/2010/secureextensions/>
			2. <http://lifehacker.com/5770947/five-best-browser-security-extensions>

- Survey the security of Android or iOS operating systems

- Survey the various forms of malware and spyware.

* + - Resources**:**
			1. Malware: Fighting Malicious Code by Ed Skoudis and Lenny Zeltser (book available on safari catalog in the library)

- Review the working of the **stuxnet worm.**

* + - Resources**:**
			1. An introductory video: <http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html>
			2. **Nicolas Falliere, Liam O Murchu and Eric Chien, W32. Stuxnet Dossier** <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>

- Benevolent Viruses (how to use viruses for beneficial purposes)

* + - Resources:
			1. Fred Cohen, A Case for Benevolent Viruses, <http://all.net/books/integ/goodvcase.html>
			2. Vojnovic, M., & Ayalvadi, G. J. (2008). On the race of worms, alerts, and patches. *IEEE/ACM Transactions on Networking, 16*(5), 1066-1079.

- Discussion of various security models: Bell-LaPadula, Biba, Clark-Wilson, Harrison-Ruzzo-Ullman, take-Grant

* + - Resources:
			1. <http://csc.uis.edu/center/resources/readings.html>
			2. <http://www.acsac.org/2005/papers/Bell.pdf>

- Give examples of both Diffie-Hellman and RSA, encrypting the same message in both system. Compare and constrast their approaches, including the practical usability of each, and their known weaknesses.

* + - Resources: book.

 - Looking at current and recent security news, choose a sub-topic and give a summary of recent and ongoing events. Look at least two weeks back in archives, and follow the news for a week.

* + - Resources:
			1. Risks forum
			2. Websites such as sans.org, slashdot.org, reddit.com (/r/netsec, /r/ComputerForensics, etc.)

- Research stack-based buffer overflows.

* + - Resources: <http://insecure.org/stf/smashstack.html>
* Bitcoin – how it works technically. Why can’t I copy my currency-file, and use it twice?

Task: Give an example of a “microbitcoin” example where you work through the exact math, except everything is just 3 digits (mod 1000): coins are merely 3-digit numbers, and person#i’s public key will be “multiply a message by the i’th prime number that doesn’t contain a multiple of 2 or 5; take that result mod 1000”. That is, person#1 mutiplies by 3 mod 1000; person#2 by 7, and person#3 by 11.

Work through the steps involved with person#1 selling coin#99 to person#2, who in turn sells it to person#3. What is the resulting coin, exactly?

* What is DNS Poisoning? What difficulties are there, in carrying it out? How can network administrators detect and stop a DNS poisoning attack?
* Code your own RSA encryption in (say) Java, without using existing cryptography libraries or code. This includes generating keys, which requires finding large prime numbers. You will want to read about (and implement) the [Miller-Rabin test](http://en.wikipedia.org/wiki/Miller%E2%80%93Rabin_primality_test) for probabilistic primality checking. Your code must be documented, and include test cases for each function. Include a 1-page write-up about how your code works, *and* what difficulties you encountered along the way. [This is substantially more work than other options, but you might find it more rewarding if you enjoy math and programming.]

“The growth of the internet in

“What is a virus? Most could agree that they are thought of to be harmful and can cause damage. Most would even say that … “

OMG: “***Abstract*--This paper is going to detail what Stuxnet is and why it is important. It is a very special kind of malware that has had a large impact on a lot of the world we currently live in. The who, what, where, why, and how about Stuxnet will be answered.**

“

In the visual representation of Fig 2, one can see the flow of requests through the kernel

One example is the interruption of routines between the user controlled application layer and the kernel. By manipulating these interrupts the user can hack into the kernel and gain unwelcome access.

*Abstract*—This is a paper on the Stunex worm for my ITEC 345 class security in computing.

# Introduction: Since the creation of technology there have been attacks on computers and other technical devices. Some attacks are minor such as hacking a friend’s Facebook and changing their profile picture. Other attacks can be more serious like identity theft. All in all, security is important in an age where technology rules the world. Viruses and worms can come from anywhere and everyone who uses technology needs some information on the different worms and viruses that exist. This paper will concentrate on one specific attack, the Stuxnet worm.

1. If you want to include any appendices with supporting material – for example the SMTP transcript demonstrated on this page – those don’t count toward the page limit either. [↑](#footnote-ref-1)