Announcements (0 minutes)
Learning Objectives for Today (1 minute)
→ How to digest an academic paper (3 minutes)
→ Understand some of the rationale for the teaching approach
→ Get some practice at developing the mindset
E-Prime for Security (5 minutes)
Hacker Curriculum Philosophy (15 minutes)
Scenarios for Security Mindset (15 minutes)
On the Infeasibility of Modeling Polymorphic Shellcode

Yingbo Song  
Dept. of Computer Science  
Columbia University  
yingbo@cs.columbia.edu

Michael E. Locasto  
Dept. of Computer Science  
Columbia University  
locasto@cs.columbia.edu

Angelos Stavrou  
Dept. of Computer Science  
Columbia University  
angel@cs.columbia.edu

Angelos D. Keromytis  
Dept. of Computer Science  
Columbia University  
angelos@cs.columbia.edu

Salvatore J. Stolfo  
Dept. of Computer Science  
Columbia University  
sal@cs.columbia.edu

ABSTRACT
Polymorphic malware remains a troubling threat. The ability for malware to automatically transform into semantically equivalent variants frustrates attempts to rapidly construct a single, simple, easily verifiable representation. We present a quantitative analysis of the strengths and limitations of shellcode polymorphism and consider its impact on current intrusion detection practice.

We focus on the nature of shellcode decoding routines. The empirical evidence we gather helps show that modeling the class of...
What is E-Prime?
What is Greenwald’s recommendation?
Do you find it compelling?
“We posit that the largely undocumented and informal Hacker Curriculum contains a number of principles and methods that can prove useful in educating undergraduates in the art of ethical computer security assessment.”
Here is a castle. Own it. Without an army.
Where Is This?
When Is This?
Texas Schools Win Right To Track Students With Creepy, Invasive RFID Locators

Adam Popescu · yesterday
Chip-and-Pin

These are unhackable, right?
// pretty good XOR encryption (but in NO way uncrackable) script
// Copyright 2001 by Terry Yuen.
// Email: kaiser40@yahoo.com
// Last update: July 15, 2001

// Encrypts a given string

function QuickSave_encrypt(str)
{
    pwd = 'locasto';
    if(pwd == null || pwd.length <= 0) {
        // alert('QuickSave Error - No encryption password given. Please contact your system
        return null;
    }
    var prand = "";
    for(var i=0; i<pwd.length; i++) {
        prand += pwd.charCodeAt(i).toString();
    }
    var sPos = Math.floor(prand.length / 5);
    var mult = parseInt(prand.charAt(sPos) + prand.charAt(sPos*2) + prand.charAt(sPos*3) + prand.charAt(sPos*4) + prand.charAt(sPos*5));
    var incr = Math.ceil(pwd.length / 2);
    var modu = Math.pow(2, 31) - 1;
    if(mult < 2) {
        // alert('QuickSave Error - Algorithm cannot find a suitable hash; bad password.
        return null;
    }
    var salt = Math.round(Math.random() * 1000000000) % 1000000000;
    prand += salt;
    while(prand.length > 10) {
        prand = (parseInt(prand.substring(0, 10)) + parseInt(prand.substring(10, prand.length)));
    }
    prand = (mult * prand + incr) % modu;
    var enc_chr = "";
    var enc_str = "";
    for(var i=0; i<str.length; i++) {
        enc_chr += parseInt(str.charCodeAt(i) ^ Math.floor((prand / modu) * 255));
    }
}
A Service

reCAPTCHA is a free anti-bot service that helps digitize books.

- WHAT IS reCAPTCHA
- GET reCAPTCHA
- PROTECT YOUR EMAIL
- MY ACCOUNT
- RESOURCES: DOCS & PLUGINS

- LEARN HOW reCAPTCHA WORKS

USE reCAPTCHA ON YOUR SITE

- STRONG SECURITY
- ACCESSIBLE TO BLIND USERS
- 30+ MILLION SERVED DAILY

NEW See how accurate reCAPTCHA is at digitizing content!

Blog | About Us | Contact | FAQs | Terms
© 2013 Google, all rights reserved.
You have a midterm exam in CPSC 525. How do you ensure a score of 100? Cheat.
I’m going to try to guess your social insurance number. Write down your SIN number, making sure to keep it private.
Guessing Game

I’m going to try to guess your social insurance number.

Write down your SIN number, making sure to keep it private.

How do you get students to write down a sensitive piece of information?
These have ethical implications, which we’ll talk about next time.
Readings are posted on the wiki. Read them for next class.