

CS642

computer
security

/introduction

adam everspaugh
ace@cs.wisc.edu

definition

Computer Security := understanding
and improving the behavior of computing systems
in the presence of **adversaries**



computing
systems

target or **victim**

adversaries



security
engineers

computer systems

- * operating systems
 - * networks, internet
 - * web browsers, web applications
 - * software applications
 - * smartphones
 - * cars: engine control systems, brakes
 - * traffic lights (industrial control systems)
 - * ...

targets



2010:
“Highly sophisticated
and targeted attack”

2011:
“Advanced persistent threat”



2011:
Bad crypto => cracked PS3
PSN is down

2014: Sony Pictures email archives stolen

security goals

- * **Confidentiality**

don't leak private information
/ encryption, access control

- * **Integrity**

no unauthorized modification of information
/ message integrity checking, access control

- * **Authenticity**

identified and accurate principles (people, computer systems)
/ digital signatures, passwords

- * **Availability**

services operating when needed
/ redundancy

adversaries



- * 31337 hax0rs — script kiddies
- * Political dissidents, insiders
- * Hacktivists
- * Professional criminals
- * National governments





attack

2011: <http://arstechnica.com/tech-policy/news/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack>

targets

Greg Hogle

owns HBGary and HBGaryFederal
runs rootkit.com



hbgaryfederal.com

rootkit.com



phase 01

/ sql injection **attack**

<http://www.hbgaryfederal.com/pages.php?pageNav=2&page=27>



usernames, password hashes

hbgaryfederal.com

Content Management System

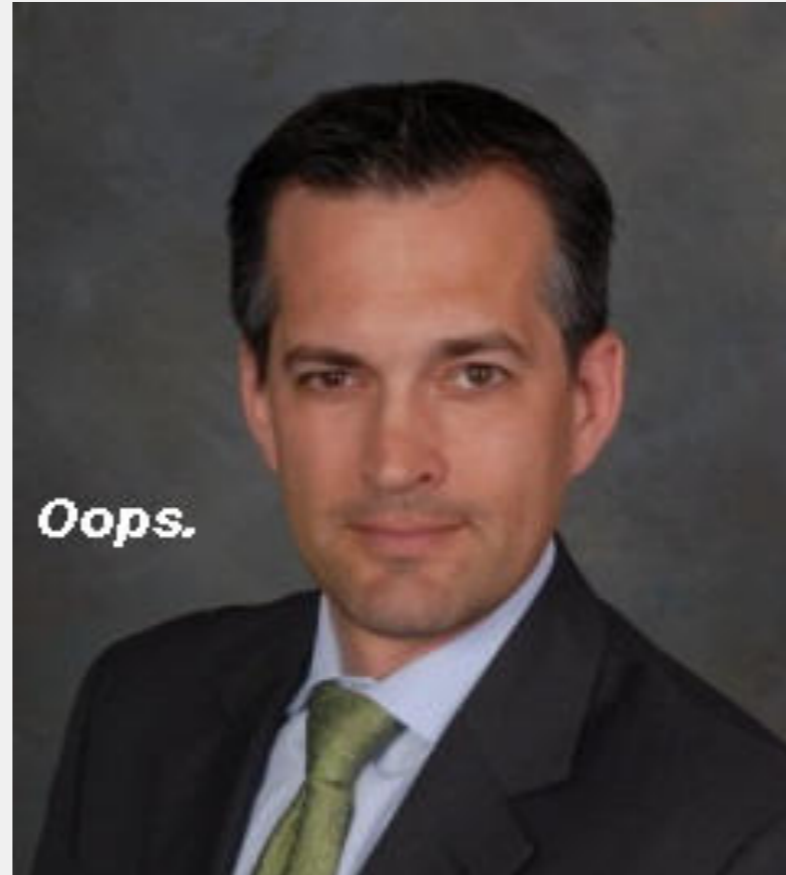
$h = \text{Hash}(pw)$

But guess-and-check works if
pw is **simple** enough

impossible to reverse

phase 02

/ password cracking



Aaron Barr (CEO)

Ted Vera (COO)

passwords had only 6 digits, lower case letters, and numbers

Tools like JohnTheRipper easily crack these passwords
in 5-10 minutes

<http://www.openwall.com/john>

phase 03

/privilege **escalation** - february 2011

```
ssh ted@support.hbgary.com --password=tedv12
```



User level account

support.hbgaryfederal.com

Exploit a privilege escalation vulnerability in the glib linker in Linux

<http://seclists.org/fulldisclosure/2010/Oct/257>

Root account: grab/delete GBs of info

phase 04



user: aaron
pass: aaro34



Google Apps



Aaron Barr -- same password on Google Apps Domain

Aaron is Google Apps administrator -- can reset passwords

Read Greg Hoglund's emails

phase 05

/social engineering

From: Greg

To: Jussi

Subject: need to ssh into rootkit

im in europe and need to ssh into the server. can you drop open up firewall and allow ssh through port 59022 or something vague?
and is our root password still 88j4bb3rw0cky88 or did we change to 88Scr3am3r88 ?


thanks



rootkit.com

recap

web security



* SQL injection

crypto



* Password cracking

Low-level software security



* Privilege escalation via setuid program

* Social engineering

You're on your own



security analysis

/ **Threat** models /

- * **Asset**

information or resource of value

- * **Threat**

mechanism used by an adversary to gain unauthorized access to an asset (context specific)

- * **Vulnerability**

flaw or defect in a computing system or design that puts an asset at risk

- * **Attack**

occurs when an adversary attempts to exploit a vulnerability

security analysis

/ **Threat** models /

- * **Compromise**

occurs when an attack is successful and adversary has access or control over a resource

- * **Threat Model**

collection of threats deemed important for a particular environment

known attacks and adversaries

security analysis

/ **Security** models /

- * **Trust Model**

all participants and computing systems (or components) that are assumed to be uncompromised and behave as expected

- * **Security Model**

countermeasures and mechanisms to improve security.
Specific to threat model + trust model.

exercise

think-pair-share

smartphone

{Threat model}

assets — attackers — vulnerabilities

{Security model}

subjects — trusted components

countermeasures — security goals

INTERMISSION

goals

- * Understand threats and **attacks**
- * Security evaluation
- * Defensive technologies
- * Advance our technical **skills**
 - * x86 assembly, low-level programming
 - * cryptography
 - * web security
 - * networking

Other **topics**: e-crime, malware, cloud computing, android,
bitcoin

ethics



think like this



act like this

> We will learn how systems **break**

> Security is an arms race
between attackers and defenders

ethics



Abuse of security vulnerabilities ...

is a violation of Univ of Wisconsin policy

<https://www.cio.wisc.edu/policies/responsible-use-information-technology-policy/>

is probably illegal

is unethical

guidelines

How do penetration testers evaluate security?

- > With explicit, written permission
 - > Must still be careful not to cause any harm

- > Homework assignments will use our own computers or virtual machines

How do we ethically study security vulnerabilities?

- > With computing systems that we own
 - > And with **ethical disclosure**

ethical disclosure

- * **Full disclosure**

/revealing everything known about a vulnerability.
Typically includes any known exploit code.

- * **Responsible disclosure**

/ensuring vendors and potential victims know about vulnerability and have time to deploy countermeasures before public disclosure

Security Update for Gray GoPayment Card Reader



intuit®

We recently learned from the University of Wisconsin, Madison about a security vulnerability with the gray GoPayment credit card reader made by our partner ID TECH. As soon as we learned about this vulnerability, we immediately started working with the university and ID TECH to test it and ensure that our GoPayment customers were not at risk.

<https://security.intuit.com/alert.php?a=051>

[2012: Frisby, Moench, Recht, Ristenpart]

- / Notified companies when draft paper was ready
- / Worked with them to ensure they could fix vulnerabilities
- / Full disclosure at workshop presentation

ethical disclosure

course details

- * Course web page
<http://pages.cs.wisc.edu/~ace/cs642-spring-2016.html>
- * Course email list for announcements
- * Grading
 - / Homework 50%
 - / Midterm 20%
 - / Final exam 20%
 - / Participation 10%
- * Most lectures: Monday, Wednesday
 - / review sessions scheduled for Fridays
 - / reserve the right to schedule make-up courses on Fridays

homework

- * 4 assignments
- * *Some* problem sets will permit teams of up to 2
- * Collaboration policy:
 - * no collaboration with people outside team
 - * using the web for general info is encouraged
 - * googling for answers to questions is not >:|
 - * cheating will be reported to university authorities
- * Need access to virtualization software

participation

- * Speak up in class
- * Engage during in-class exercises
- * Recommend:
 - / skim readings before lecture
 - / read in-depth later on topics of interest

office hours

89 students: 1 instructor



very bad odds for handling email

I may not answer emails, or I may ask you to come to office hours -- when in doubt, just come to office hours

Office hours:
Fridays 2:30-3:30p

exit slips

- * Take 1-2 minutes to reflect on this lecture
- * On a partial-sheet of paper write:
 - / One thing you learned in this lecture
 - / One thing you didn't understand