

Intro

Monday, July 15, 2013
8:27 AM

Melissa
from Bakersfield (BHS)

Alfonso

Operational Security

Securing systems & networks - "free time" on Thurs afternoons
Users, authentication, access control
Social Engineering

Format

Morning

2 sessions

9:00 ~ 10:15

10:30 ~ noon

Lunch

noon ~ 1:30

Afternoon

Hands-on sessions and/or detailed lectures

Surveys & Contact Info

Ethics & Legality

Must have strong ethical background

Legal framework

Federal - criminal & civil

State - criminal & civil

Basic safeguards

permission is key

maintain boundaries

avoid liabilities

Ethics

many codes of ethics from professional societies

• Kern ISSA
(ISC)²
CompTIA
ISACA

What is security?

Traditional

Confidentiality

Integrity

Availability

Generalized

Threats / Risks / Vulnerabilities

Prevention / Mitigation

Response

Awareness

Risk / Benefit analysis

Threats → Risks → Costs → Benefits

acceptable level of risk

mitigation / prevention plan
"best practices"

Operational Security

Physical security matters

Identity in a computer system

"Entity" or "role-based" identity

User database

username, authentication method

Auth methods

Something you know

Something you have

Something you are

Password Storage

Plain text

Hashed - One way encryption

Easy: password → hash

Hard: hash → password

Letters & Numbers | Example: password has 6 letters (lowercase)

Letters & Numbers

$$26^6 = 2,176,782,336$$

$$\frac{2,176,782,336}{1,000,000} = 2177 \text{ seconds} \sim 36 \text{ min}$$

$$\frac{2,176,782,336}{20,000,000} = 108 \text{ seconds}$$

Example! password has 6 letters (lowercase)

$$\underline{26} \cdot \underline{26} \cdot \underline{26} \cdot \underline{26} \cdot \underline{26} \cdot \underline{26} \rightarrow 26^6 = 308,915,776$$

1 million guesses/sec

$$\frac{308,915,776}{1,000,000} = 309 \text{ seconds} \sim 5 \text{ minutes}$$

20 million guesses/sec

$$\frac{308,915,776}{20,000,000} = 15 \text{ seconds}$$

Upper Case, Lower Case & Numbers

$$6 \text{ characters} \quad 62^6 = 56,800,235,584$$

$$1 \text{ million/second} \rightarrow 56800 \text{ seconds} \rightarrow 946 \text{ minutes} \rightarrow 15.7 \text{ hours}$$

$$20 \text{ million/second} \rightarrow 2840 \text{ seconds} \rightarrow 47 \text{ mins}$$

$$10 \text{ characters} \quad 62^{10} = 839,299,365,868,340,224$$

$$1 \text{ million/second} = 839299365868 \text{ seconds} \\ 13988322764 \text{ mins} \\ 9714113 \text{ days}$$

$$20 \text{ million/second} = 41964968293 \text{ seconds} \\ 485,706 \text{ days}$$

$$500 \text{ million/second} = 1,678,548,731 \text{ seconds} \\ 19,428 \text{ days}$$

Factors That Affect Password Difficulty

Length of password (exponent)

Characters chosen for password (base)

random choosing

Factors That Affect Guess Rate

Types of passwords (e.g. dictionary is easy)

Hash Algorithm

how the computer turns the password into a hash

Processors available

more cores $\rightarrow$ more guesses

CPU crackers use the general purpose processor

cores can do multiple computations

have multiple cores to divide workload

GPU crackers use the graphical processor

allows many more simultaneous calculations

	Alg	1 card (6990)	25 cards
"fast"	NTLM	7-9 billion/sec	350 billion/sec
	MD5	5-7 billion/sec	180 billion/sec
	SHA1	2-3 billion/sec	63 billion/sec
"slow"	Bcrypt	4,000 /sec	71,000 /sec
	SHA512crypt	12,000-18,500 /sec	364,000 /sec