PASSWORDS

THE GOOD, BAD, & THE UGLY

SCOTT G. AINSWORTH
FOR GRADUATE TEACHING ASSISTANT INSTITUTE
JANUARY 11, 2012
OVERVIEW

• The problems with Passwords
• A Better Alternative
• Then why do we still have them?
• Run as fast as you can!
• If you must use a password…
THE PROBLEMS WITH PASSWORDS

A Little Recent History

• Jun ’11 Sony 77M
• Jan ’12 Zappos 24M
• Jan ‘12 Dropbox “thousands”
• Jun ’12 LinkedIn 6.5M
• Aug ’12 Blizzard millions
• Nov ’12 Twitter millions
25-GPU MONSTER

42 Trillion Guesses since I started talking

350 Billion Guesses per Second

$250K

Scott G. Ainsworth • January 11, 2013 • ODU GTAI
CloudCracker

An online password cracking service for penetration testers and network auditors who need to check the security of WPA protected wireless networks, crack password hashes, or break document encryption.

"Welcome to the future: cloud-based WPA cracking is here!"
-- TechRepublic

"Low cost service cracks wireless passwords from the cloud..."
-- TheRegister

"This really is a great idea."

A BETTER ALTERNATIVE

- Two-Factor Authentication
  - Something you know
  - Something you have
WHY DO WE STILL USE THEM?

• Simply put…
  It’s about…
  Money…

• It’s cheaper to react…
  Than to adapt…
RUN AWAY, RUN AWAY!

- For vital services
  - Email
  - Banking
- Demand two-factor authentication
- If they won’t change, leave
IF YOU MUST USE A PASSWORD...

- Good  !HeWf5nPbuN0C|.avafCn
- Bad    TBoNTBtItQ#0
- Ugly   KateBrian

- Use a password manager
  - Roboform
  - 1Password
  - PassKey
IF YOU MUST USE A PASSWORD...

A really strong password is one that nobody else has ever used.

— Joseph Bonneau
WRAP UP

• The time of passwords is over
• Use two-factor authentication — switch if you have to
• Use a password manager
REFERENCES

• Bonneau, Joseph. “Want to create a really strong password? Don’t ask Google.”


• Gamache, Mark. “NTLM Challenge Response is 100% Broken.”

• Goodin, Dan. “25-GPU cluster cracks every standard Windows password in <6 hours.”


• Perlroth, Nicole. “How to Devise Passwords That Drive Hackers Away.”

• Schneier, Bruce. “Passwords aren’t broken, but How We Choose them Still is.”