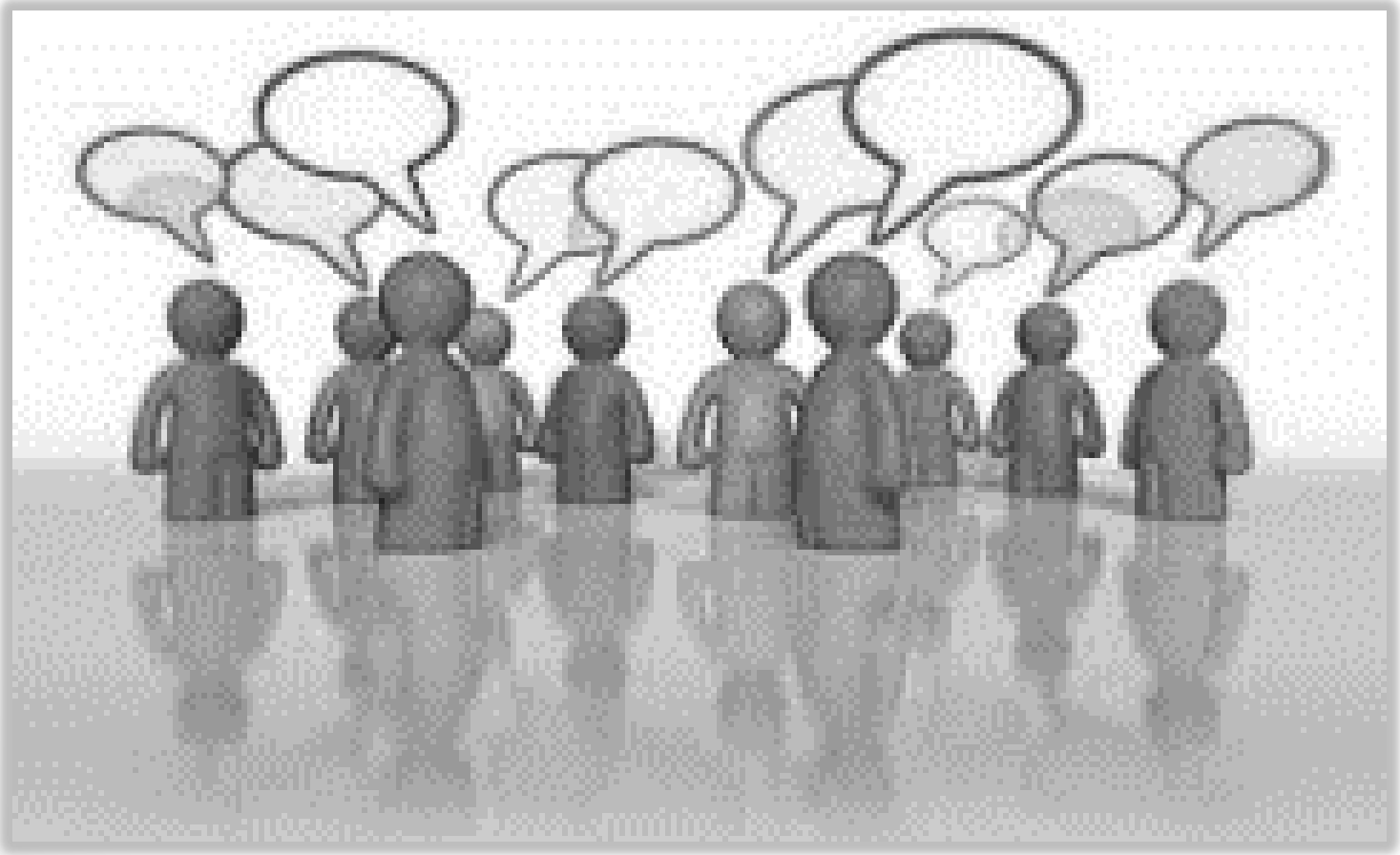
# Cybersecurity

## SEIDENBERG SCHOLARS SUMMER EXPERIENCE 2014

Andreea Cotoranu July 2014

# Personal stories from the tranches

- Share a story about a security incident that happened to you or someone you know



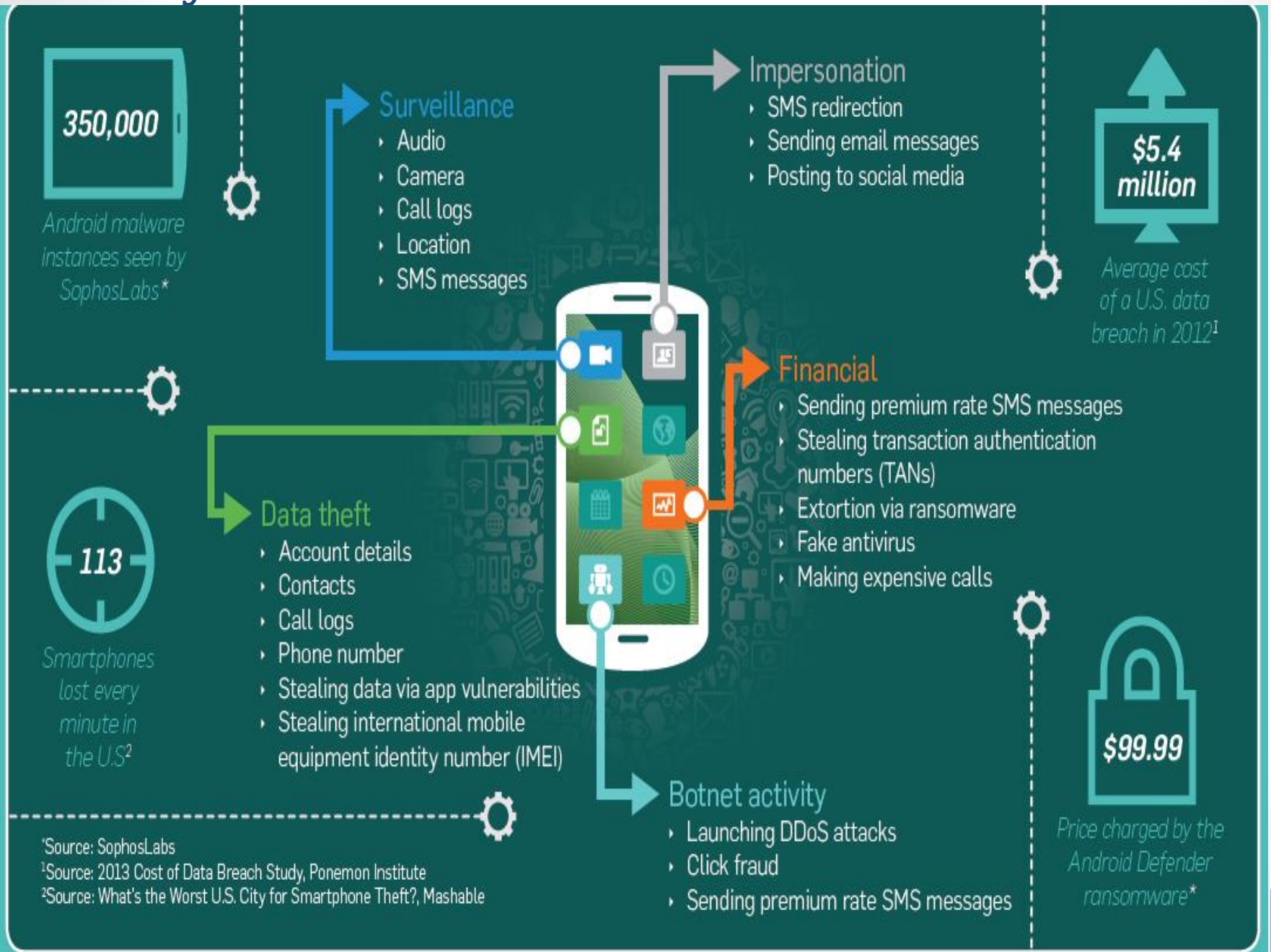
# Other stories from the tranches

- Everything around us is under attack: cars, medical devices, smartphones, fitness devices, water treatment systems, social networking sites, ATMs, governments, children toys, and the list continues…

*Karotz Your Smart Rabbit*

*http://store.karotz.com/en_US/*

# Story I: Android Malware



# Story II: GameOver/Zeus (GOZ) Malware

## BUILDING THE BOTNET

Cyber criminals create a network of compromised computers by sending emails with embedded malicious links or attachments or by enticing users to visit infected websites. Once infected, covertly installed malware connects computers to the botnet infrastructure without the owners' knowledge.

## COMMAND AND CONTROL SERVERS

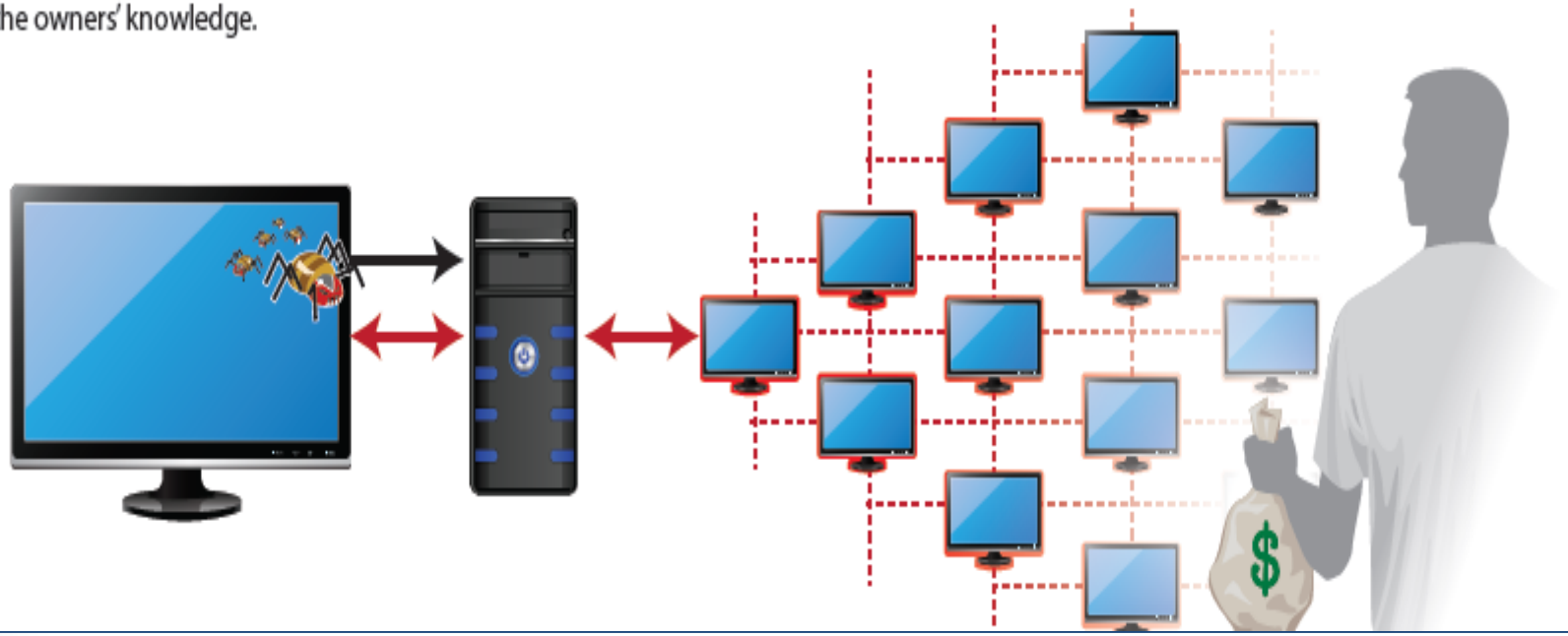
At the core of the botnet are servers which issue commands orchestrating various criminal activities.

## BOTNET USE

Infected computers are organized together to implement illicit orders from the command and control servers.

## A QUIET THREAT

Botnets typically operate without obvious visible evidence and can remain operational for years.



GOZ malware can be used to download and install additional malware, including Cryptolocker, as well as extract banking credentials, which facilitates the illegal withdrawal of funds from individuals and businesses through financial institutions. The criminals' ability to access accounts at will undermines business integrity and public confidence and has the potential to threaten financial infrastructure.

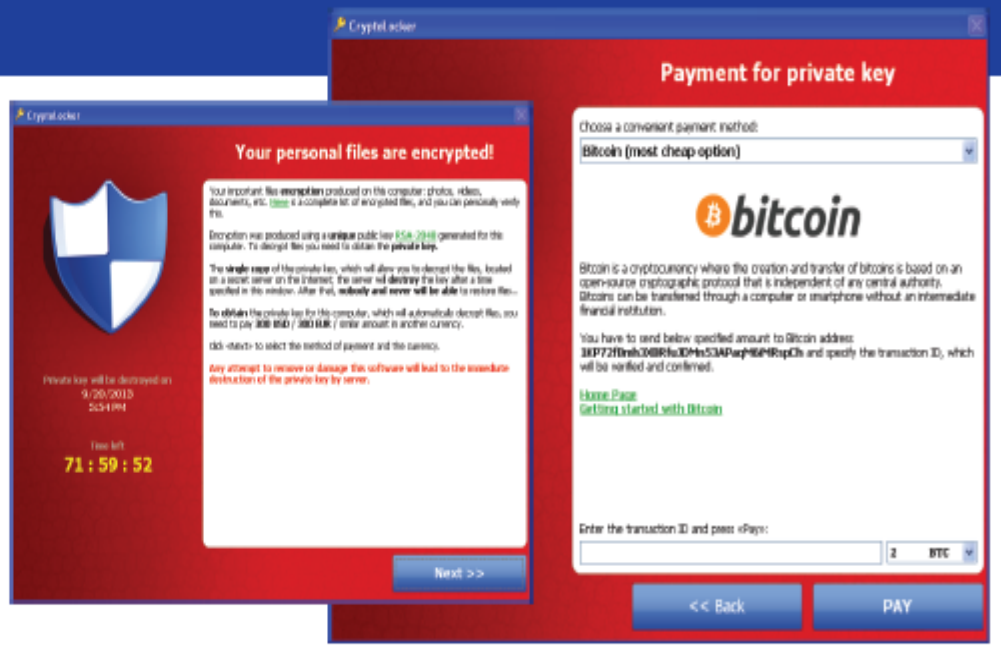
Source: http://www.fbi.gov/news/stories/2014/june/gameover-zeus-botnet-disrupted/gameover-zeus-botnet-disrupted

# Story II: GameOver/Zeus (GOZ) Malware (contd.)

## CryptoLocker Malware

Computers compromised by the GOZ botnet may also be infected with CryptoLocker, a form of "ransomware."

- Victim files are encrypted and held "hostage" until the victim makes payment
- More than 121,000 victims in the United States and 234,000 victims worldwide
- There were approximately $30 million in ransom payments between September and December 2013




## GOZ/CryptoLocker Scope

- More than 1 million GOZ infections globally
- Roughly 25% of infected computers are located in the United States
- Losses estimated globally in the hundreds of millions of dollars
- Key participation of 10 partner countries in support of takedown operation

Source: http://www.fbi.gov/news/stories/2014/june/gameover-zeus-botnet-disrupted/gameover-zeus-botnet-disrupted

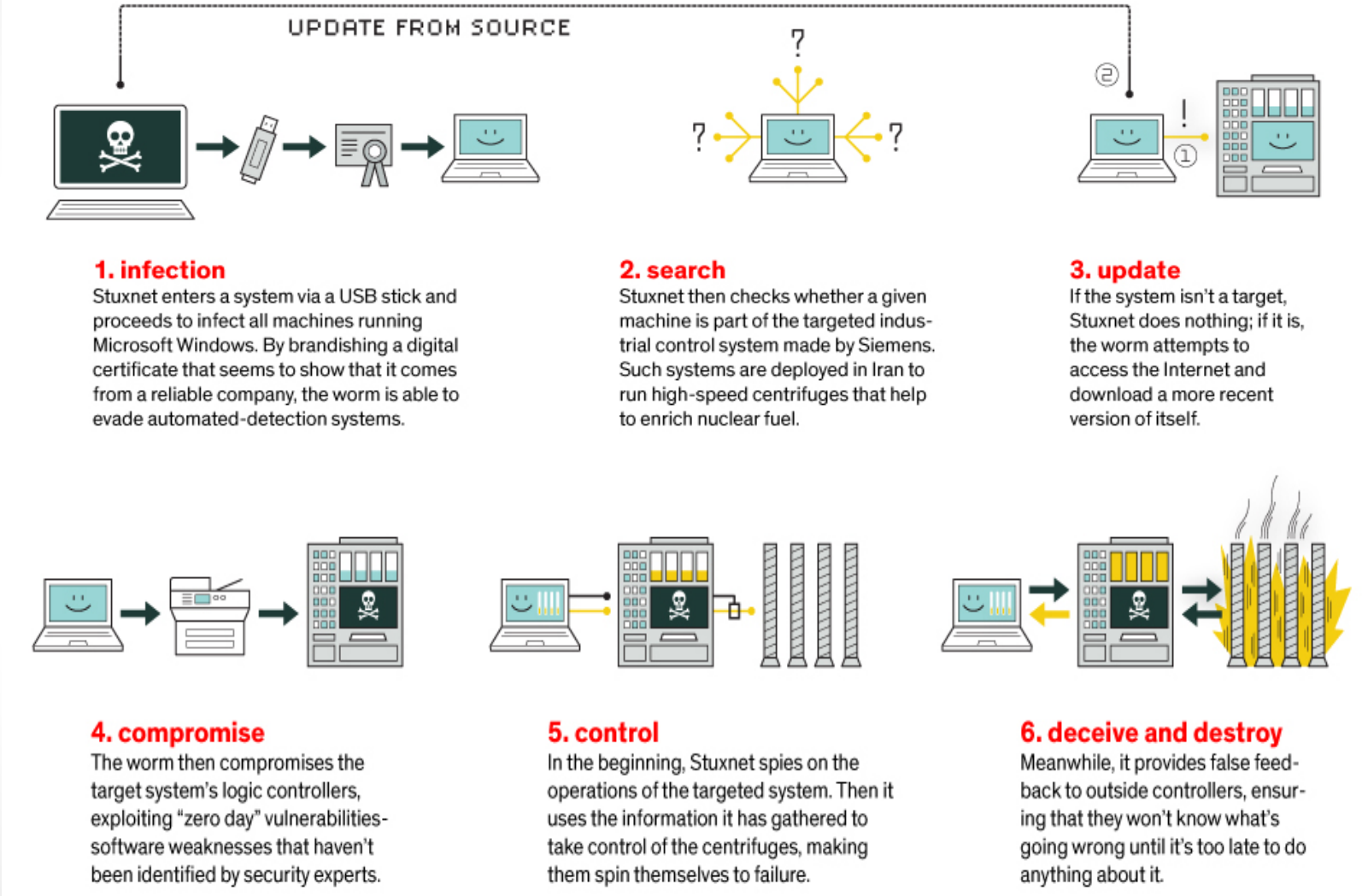
# Story III: Stuxnet

- The first publicly disclosed cyber weapon continues to amaze everyone from military strategists and computer security experts, to political decision-makers and the general public.

- Watch Video:

http://www.youtube.com/watch?v=DSMOs7CF1Eo&list=PLtkZe73xAAKT9mjqFGKoLZY_szzuGcQSs

# Story III: Stuxnet




Source: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

# Ethics - Ten Commandments

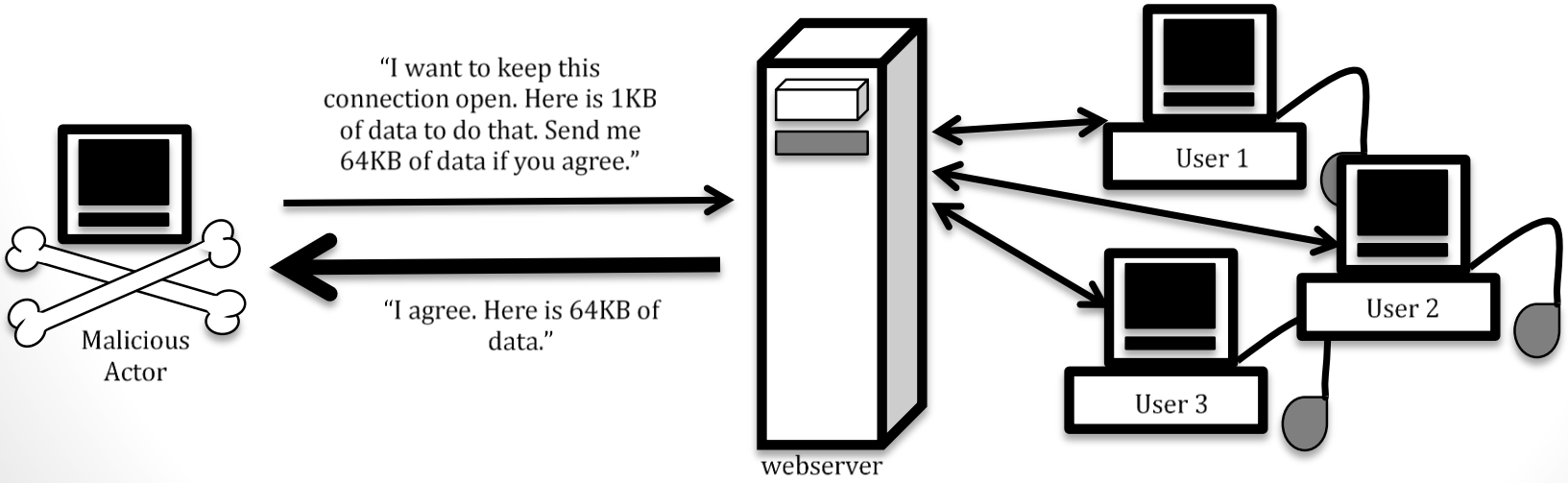
- Thou Shalt Not
  - Use a Computer to Harm Other People
  - Interfere With Other People's Computer Work
  - Snoop Around in Other People's Computer Files
  - Use a Computer to Steal
  - Use a Computer to Bear False Witness
  - Copy Or Use Proprietary Software for Which You Have Not Paid
  - Use Other People's Computer Resources Without Authorization or Proper Compensation
  - Appropriate Other People's Intellectual Output
  - Think About the Social Consequences Of The Program You Are Writing Or the System You Are Designing
  - Always Use a Computer in Ways That Insure Consideration and Respect For Your Fellow Humans

Adapted from Source: http://cpsr.org/issues/ethics/cei/

# BREAK

# Heartbleed – one of the biggest stories of 2014

- SSL/TLS - security protocols used to encrypt and secure Internet traffic; websites that use “https” use SSL/TLS;
- OpenSSL - open source toolkit for SSL/TLS implementation;
- Heartbeat extension - sends a small request to and receive a small amount of data from a webserver to keep a connection between the user’s computer and the webserver live;




Source: MS-ISAC

# Heartbleed – Let's Play It Out!

- Actors:
  - Webserver
  - Eve the Malicious User
  - Other Users

# P@$$wOrd$

# Authentication

- Prove that you are who you say you are in order to gain access to a resource
- **Something you know (eg. a password)**
- Something you have (eg. a smart card)
- Something you are (eg. a fingerprint)
  - Pace U is researching biometric authentication

# Passwords: Advantages and Disadvantages

- Advantages
  - Simple to implement
  - Straightforward to revoke or change
  - Easy for users to understand
  - Allow for quick authentication
- Disadvantages
  - Difficult for users to create an remember passwords that are hard for an attacker to guess

# Passwords: Entropy

- Entropy estimates the strength of a password
  - Higher entropy = Stronger password

- Entropy measures the number of bits it would take to represent every password of length L under an alphabet of N different symbols

$$\mathbf{H = L \log_2 N}$$

- Examples of password entropy values:
  - example (7 lower-case characters)
    - entropy H = $7 \log_2 26 \sim 32.9$ bits
  - *P4ssw0Rd14* (10 alpha-numeric characters)
    - entropy H = $10 \log_2 62 \sim 59.54$ bits

# Exercise: Which password is stronger?

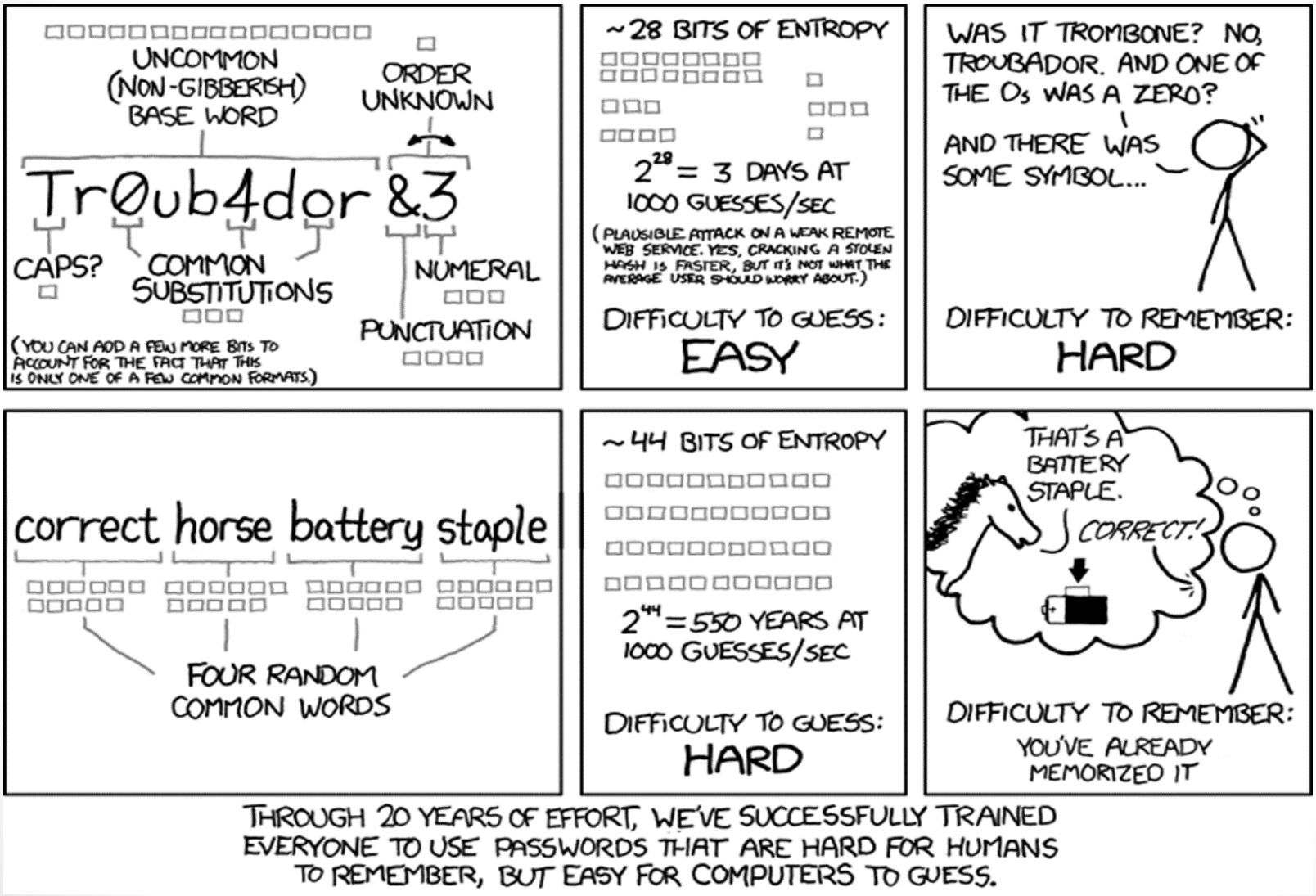
- Discuss in teams
- Count votes
- Reveal answer

# Exercise: Which password is stronger? Answer:

- Password I:
  - F#Mo1e*TJC8
  - entropy H = 12 $\log_2$ 72 ~ 74 bits
- Password II:
  - carrot ways base split
  - entropy H = 22 $\log_2$ 27 ~ 104.61 bits

Source: http://blog.shay.co/password-entropy/

# Passwords: How to choose a good one?




Source: Password Strength by Randall Munroe, http://xkcd.com/936/

# Passwords: Difficult to make a choice!

- Password Rant:
  - http://www.youtube.com/watch?v=jQ7DBG3ISRY

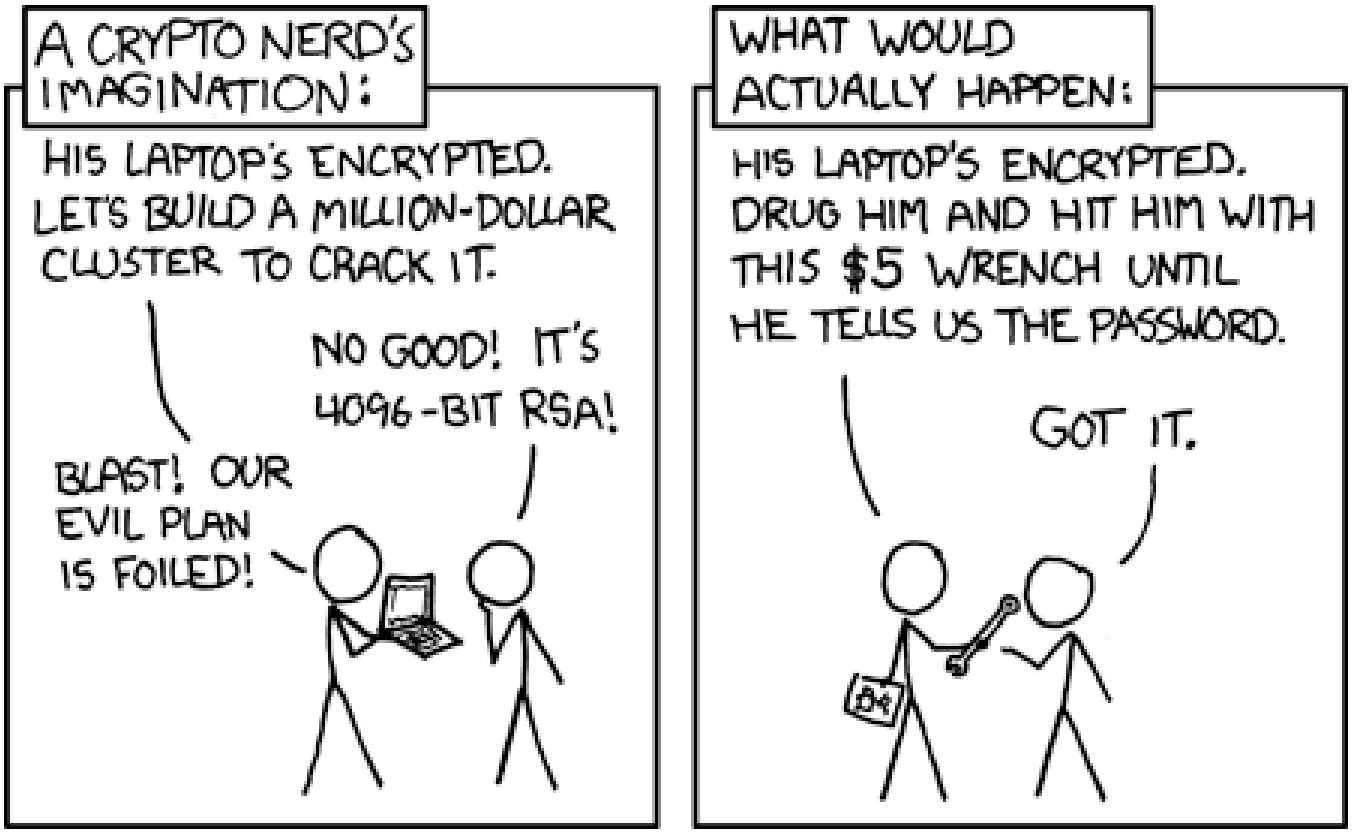
# Passwords: Better Choices Anyone?

- **Password manager**
- **Android L's 'personal unlocking‘**
- **Digital ink**
- **Password pills**

# Exercise: Crack the Combination Lock

- Each team gets one lock
- Two rounds / team
- 3 minutes / round
- Prize for the first crack in each round
- Locks will stay around for those keen on cracking the combination(s)

# Approaches to solving a security problem




Source: http://xkcd.com/538/

# Read for Fun:

How elite security ninjas choose and safeguard their passwords

http://arstechnica.com/security/2013/07/how-elite-security-ninjas-choose-and-safeguard-their-passwords/

**It's official: Malicious hackers have crappy password hygiene, too**

http://arstechnica.com/security/2014/06/its-official-malicious-hackers-have-crappy-password-hygiene-too/

# Questions?