
Digital Security:

Train the Trainer

Lindsay Beck
National Democratic Institute
@becklindsay
@NDItch

Jessie Posilkin
Legal Services Corporation
@jposi
@lsc_Tweets

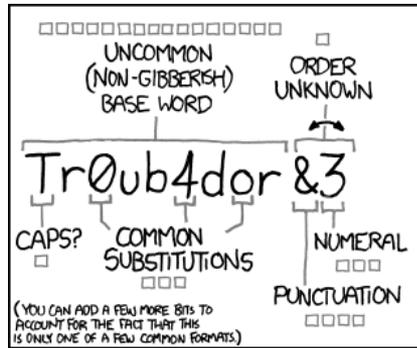
Today's Agenda

- Basics of Risk Assessment
 - Activity: Information Mapping
 - Strong Passwords
 - Browsing Safety
 - Activity: Secure Postcards
 - Mobile Security
 - Travel Security
-

Basics of Risk Assessment: Information Mapping

- Where do you store Information?
 - What do you store there?
 - How sensitive is it?
-

Password Security



~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

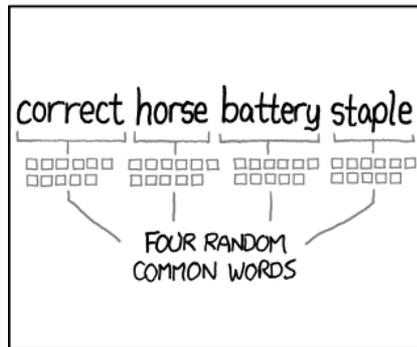
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE O's WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: **HARD**



~44 BITS OF ENTROPY

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: **HARD**

THAT'S A BATTERY STAPLE.

CORRECT!

DIFFICULTY TO REMEMBER: **YOU'VE ALREADY MEMORIZED IT**

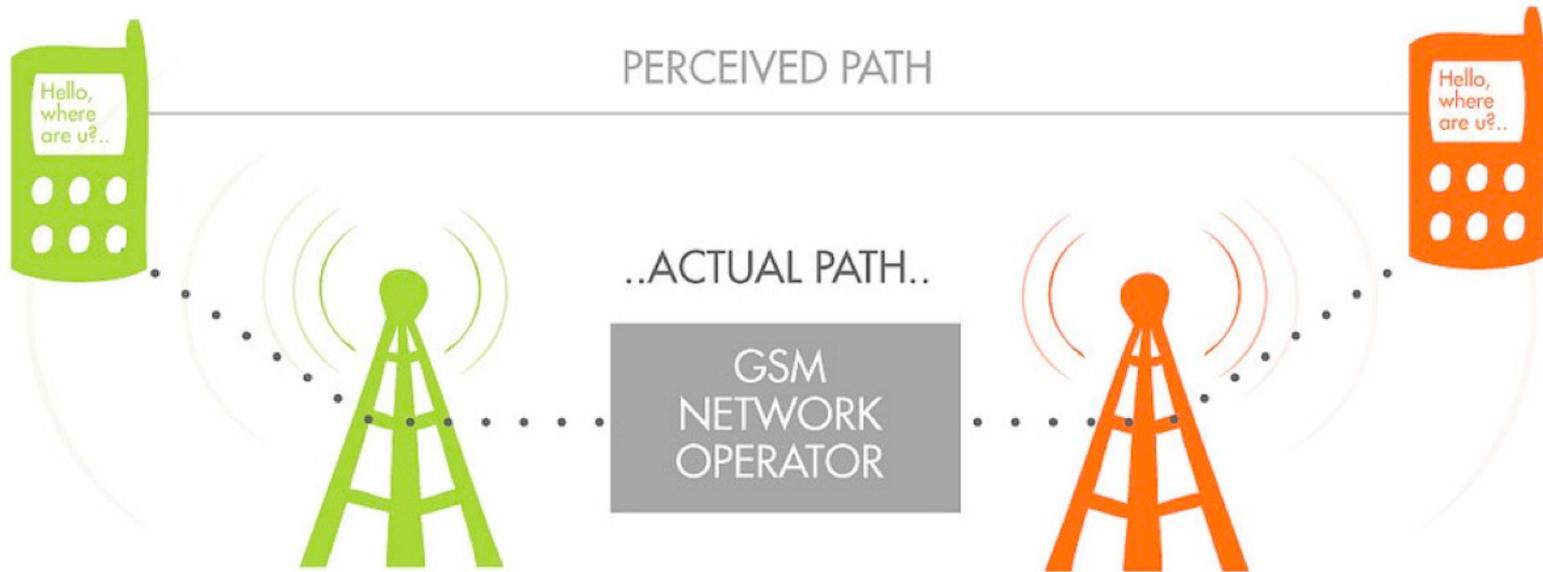
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Basic Browsing Safety:

Send a Letter, Not a Postcard

Basic Phone Security:

What is a network?



Travel Security: Checklists

- **Before you Leave**
 - **While You Travel**
 - **When You Return**
-

Passwords

- First step in accessing any web-based content, if a password is discovered by a malicious actor then your data and communications can become compromised
- General recommendations:
 - Length: at least 8 characters
 - Strength: diversity of characters (letters/symbols, and whether they are upper case or lower case)
 - Rotation: they should be changed on a semi-regular basis
 - Uniqueness: do not repeat the use of passwords
 - More frequent rotation - prioritization (important ones change more often)
 - also situational - change after risky experience
 - From trusted computer!
- Extremely difficult to follow these practices on your own
 - Multi-word passphrases solution

<p>UNCOMMON (NON-GIBBERISH) BASE WORD</p> <p>ORDER UNKNOWN</p> <p>Tr0ub4dor&3</p> <p>CAPS? COMMON SUBSTITUTIONS NUMERAL PUNCTUATION</p> <p>(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)</p>	<p>~28 BITS OF ENTROPY</p> <p>$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$</p> <p>(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)</p> <p>DIFFICULTY TO GUESS: EASY</p>	<p>WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?</p> <p>AND THERE WAS SOME SYMBOL...</p> <p>DIFFICULTY TO REMEMBER: HARD</p>
<p>correct horse battery staple</p> <p>FOUR RANDOM COMMON WORDS</p>	<p>~44 BITS OF ENTROPY</p> <p>$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$</p> <p>DIFFICULTY TO GUESS: HARD</p>	<p>THAT'S A BATTERY STAPLE.</p> <p>CORRECT!</p> <p>DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT</p>

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

On the Road: Digital Security when Traveling

- **Types of behavior when traveling:**
 - Have to carry your devices with you, may be investigated at border crossings
 - May access untrusted or public wifi connections
- **Why this matters:**
 - Device can be stolen
 - Open network can be a vector for malware or stealing login credentials
- **What should I do when I'm in transit?**
 - **Carry as little data as possible:** Travel with a “clean” device that contains only the information you need for a particular trip, and then securely delete those files before returning to the United States.
 - **Keep a backup of your data elsewhere:** Someone could seize your laptop, phone, or other devices for no reason at all. You should be prepared for the possibility that you could be deprived of access your data for some time, and store copies somewhere else that you can easily access if your devices are taken from you.
 - **Securely store the data on your device.** Many devices such as laptops and phones give you the option to set a password, numeric PIN, or other authentication method to control access to your data. Take advantage of this security feature to give your data a little more protection.
 - Use the Swype function on your Android to lock your device? You should change to a password instead, because it is very easy to see the pattern when it's held near a light.
 - Remember to shut down your device completely before traveling. This prevents someone from more easily being able to gain unauthorized access to your computer.
 - **Require screensaver logins too!** Set the screensaver on your system to start automatically after a short time (such as 2 or 5 minutes) and to require that the user supply their password again before the screensaver will unlock.
- **What should I do when I want to use my device?**
 - **Turn off Wi-Fi.** When you're not using your Wi-Fi connection on any of your devices, it's good practice to turn it off. That way it won't automatically connect to any Wi-Fi that is in the area. And for your mobile devices, it will help save your battery life since your mobile will not be constantly searching for an available Wi-Fi connection.
 - **Log out of email, social media sites, etc.** When you connect to an untrusted network, and you are already signed in, it is much easier for a hacker to gain access to your account than when you are signed out.
 - **Connect to as secure of a wifi network as possible** If the wifi network you are accessing has a password, it is much better to connect to this than an open network. You can tell when a network is not secured because you will see a message when you connect saying that you are “connecting to an unsecured

network”, or it will not have a lock next to it in the wireless connections menu. And if you are using an unsecured network, do not conduct any sensitive activities online (online banking, etc.)

- **Only use HTTPS** HTTPS, or hypertext transfer protocol (HTTP) with secure sockets layer (SSL, hence the S after HTTP), is a more secure option set up by a website owner who knows security is essential. Look for “HTTPS://” in the address bar to signify you are on a secure page. Even on an open, unsecured wireless connection, HTTPS is more secure than HTTP.
- ***When you return home:***
 - **Run your antivirus program** before you reconnect to your home network
 - **Change passwords**, especially to any accounts you may have accessed when traveling, such as email.

How do mobile networks work?

- The SIM card has a unique number - the **IMSI** - that is stored as a 64-bit field in the SIM inside the phone and is sent by the phone to the network.
- Your handset has a unique number, the **IMEI**
- Cell towers relay information from your phone to the Mobile Network Operator (MNO)
- Cell towers “triangulate” your location and relay data to and from your phone

The Network: Transmitting Information



Monday, May 21, 2012

Mobile Network Operators:

- Sells you a SIM card
- Owns or leases cell towers
- Relays data to/from your phone
- Stores your data (call logs, SMSs, triangulation)
- Charges you

What should I do?

- **Device protection:**
 - Password protect your mobile device
 - Put a pin on your SIM card
 - Remove battery from phone when not in use
- **Limit data stored on phone:**
 - Clear call logs
 - Limit number of stored contacts
 - Delete SMS and MMS threads, and reduce storage maximum (default is usually 200 SMS and 10 MMS)
 - Don't save outbound SMS

- Email or transfer sensitive media to a PC and upload securely from there
- **Limit accessibility:**
 - Turn off Bluetooth and WiFi unless actively using them
 - Avoid open and unencrypted WiFi networks
 - Always use HTTPS when on a WiFi network, and look for a lock icon in your browser
 - Use strong passwords for online accounts; and sign out of applications when not being used
 - Evaluate apps carefully: check to see what permissions they have. Install only apps you really need
-

Information Mapping and Sensitivity Ranking Worksheet

Instructions: List each type of information or data you have in each of these places. Examples of such data include: Email, Contact details, Reports/research, Accounts/spreadsheets, Videos, Images, Private messages on Facebook, etc. For data stored in more than one place, you can specify whether it is a “Master” copy, or a “Duplicate”. For example, your “Master” copy of email could be in the cloud (if you use web-based email), and “Duplicates” can be listed under Computer Hard Drive (if you use a mail client like Outlook), Smartphone, etc.

To determine the sensitivity of each type of data, please consult the following page:

	Computer Hard Drive	USB / External Hard Drive	Cloud Storage	Smartphone	Print	Other
High Sensitivity						
Medium Sensitivity						
Low Sensitivity						

Information Mapping and Sensitivity Ranking Worksheet

Instructions: For each piece of data, ask the following questions listed below for each column. If ALL of the above answers are A/B (GREEN), rating is LOW; if ANY of the above answers are C (YELLOW) and NONE are D (RED), rating is MODERATE; if ANY of the above answers are D (RED), rating is HIGH

SCALE: A/B = GREEN = LOW C = YELLOW = MODERATE D = RED = HIGH

CONFIDENTIALITY QUESTIONS	INTEGRITY QUESTIONS	AVAILABILITY QUESTIONS
1. Does the information include or contain PPSI (Personal, Private, or Sensitive Information)? A) No - continue with Confidentiality questions D) Yes - Confidentiality is High (rate below), continue with Integrity questions	1. Does the information include personnel / HR records? A) No - continue with Integrity questions D) Yes - Integrity is High (rate below), continue with Availability questions	1. Is availability of the information essential for any emergency response or disaster recovery? A) No - continue with Availability questions D) Yes - Availability is High (rate below)
2. What impact does unauthorized access or disclosure of information have on health and safety? A) None - continue with Confidentiality questions B) Minimal impact - continue with Confidentiality questions C) Limited impact - continue with Confidentiality questions D) Severe Impact - Confidentiality is High (rate below), continue with Integrity questions	2. Is the information (e.g., security logs) relied upon to make critical security decisions ? A) No - continue with Integrity questions D) Yes - Integrity is High (rate below), continue with Availability questions	2. This information needs to be provided or available: A) As time permits - continue with Availability questions C) Within 1 to 7 days - continue with Availability questions D) 24 hrs. per day/7 days a week - Availability is High (rate below)
3. What is the financial impact of unauthorized access or disclosure of information? A) None - continue with Confidentiality questions B) Minimal impact - continue with Confidentiality questions C) Limited impact - continue with Confidentiality questions D) Severe Impact - Confidentiality is High (rate below), continue with Integrity questions	3. What impact does unauthorized modification or destruction of information have on health and safety of the organization's staff or partners? A) None - continue with Integrity questions B) Minimal impact - continue with Integrity questions C) Limited impact - continue with Integrity questions D) Severe Impact - Integrity is High (rate below), continue with Availability questions	3. What is the impact to the organization's staff or partner health and safety if information were not available when needed? A) None - continue with Availability questions B) Minimal impact - continue with Availability questions C) Limited impact - continue with Availability questions D) Severe Impact - Availability is High (rate below)
4. What impact does unauthorized access or disclosure of information have on the organization's mission? A) None - continue with Confidentiality	4. What is the financial impact of unauthorized modification or destruction of information? A) None - continue with Integrity questions B) Minimal impact - continue with Integrity	4. What is the financial impact if information were not available when needed? A) None - continue with Availability questions B) Minimal impact - continue with Availability

Information Mapping and Sensitivity Ranking Worksheet

<p>questions B) Minimal impact - continue with Confidentiality questions C) Limited impact - continue with Confidentiality questions D) Severe Impact - Confidentiality is High (rate below), continue with Integrity questions</p>	<p>questions C) Limited impact - continue with Integrity questions D) Severe Impact - Integrity is High (rate below), continue with Availability questions</p>	<p>questions C) Limited impact - continue with Availability questions D) Severe Impact - Availability is High (rate below)</p>
<p>5. What impact does unauthorized access or disclosure of information have on public or partner trust? A) None - continue with Confidentiality questions B) Minimal impact - continue with Confidentiality questions C) Limited impact - continue with Confidentiality questions D) Severe Impact - Confidentiality is High (rate below), continue with Integrity questions</p>	<p>5. What impact does unauthorized modification or destruction of information have on the organization's mission? A) None - continue with Integrity questions B) Minimal impact - continue with Integrity questions C) Limited impact - continue with Integrity questions D) Severe Impact - Integrity is High (rate below), continue with Availability questions</p>	<p>5. What is the impact to the organization's mission if information were not available when needed? A) None - continue with Availability questions B) Minimal impact - continue with Availability questions C) Limited impact - continue with Availability questions D) Severe Impact - Availability is High (rate below)</p>
<p>6. Is confidentiality mandated by law or regulation? If yes, determine the impact of unauthorized access or disclosure of information. A) No - continue with Confidentiality questions B) Yes - Minimal impact - continue with Confidentiality questions C) Yes - Limited impact - continue with Confidentiality questions D) Yes - Severe impact - Confidentiality is High (rate below), continue with Integrity questions</p>	<p>6. What impact does unauthorized modification or destruction of information have on public or partner trust? A) None - continue with Integrity questions B) Minimal impact - continue with Integrity questions C) Limited impact - continue with Integrity questions D) Severe impact - Integrity is High (rate below), continue with Availability questions</p>	<p>6. What is the impact to public or partner trust if the information were not available when needed? A) None - see Instructions below B) Minimal impact - see Instructions below C) Limited impact - see Instructions below D) Severe impact - Availability is High (rate below)</p>
<p>7. Is the information intended for limited distribution? If yes, determine the impact of unauthorized access or disclosure. A) No - continue with Confidentiality questions B) Yes - Minimal impact - continue with Confidentiality questions C) Yes - Limited impact - continue with Confidentiality questions D) Yes - Severe impact - Confidentiality is High (rate below), continue with Integrity questions</p>	<p>7. Is integrity addressed by law or regulation? If yes, determine the impact of unauthorized modification or destruction of information. A) No - continue with Integrity questions B) Yes - Minimal impact - continue with Integrity questions C) Yes - Limited impact - continue with Integrity questions D) Yes - Severe impact - Integrity is High (rate below), continue with Availability ques.</p>	

Information Mapping and Sensitivity Ranking Worksheet

<p>8. Is the information publicly available? A) No - see Instructions below, then continue with Integrity questions B) Yes - see Instructions below, then continue with Integrity questions</p>	<p>8. Is the information (e.g., financial transactions, performance appraisals) relied upon to make business decisions? If yes, determine the impact of unauthorized modification or destruction of information. A) No - see Instructions below then continue with Availability questions B) Yes - Minimal impact - see Instructions below then continue with Availability ques. C) Yes - Limited impact - see Instructions below then continue with Availability ques. D) Yes - Severe impact - Integrity is High (rate below), continue with Availability ques.</p>	
---	---	--

<p>CLASSIFICATION RATING FOR CONFIDENTIALITY:</p>	<p>CLASSIFICATION RATING FOR INTEGRITY:</p>	<p>CLASSIFICATION RATING FOR AVAILABILITY:</p>
---	---	--