# Data Privacy and Security on the Web

Li-Chiou Chen

Seidenberg School of Computer Science and Information Systems Pace University March 28<sup>th</sup>, 2014

#### Agenda

- Web privacy
- Embedded privacy information
- Web transaction security
- Cybersecurity awareness resources
- PCAP summer project

#### What are things you do on the web?





© Li-Chiou Chen, Pace University

Do I care about my privacy on the web? How it is handled?



What is privacy? What is web privacy?

- Privacy
  - "the control an individual has over information about himself or herself"
  - a social and cultural concept
- Web privacy
  - The right of Web users to conceal their personal information
  - Web users have some degree of control over the use of any personal information disclosed to others

#### Activity I: Examine Privacy Statement

- Go to www.facebook.com
- Click on "privacy" at the bottom of the page
- You will see "Data Use Policy" on the next page
- Read the section on "Information that is always publicly available"
- Do you know these before?

When I post information (e.g. pictures) on the web, am I giving away any privacy information?



#### Privacy information hidden in the data

Pictures

Files

Web pages

. . . . .

#### Explore / Tags / flicker

Sort by: Most recent • Most interesting

flicker clusters Explore and refine this flicker list with our wonderful clustery

bird, flame, woodpecker, candle, northernflicker, light, birds, nature, colaptesauratus, northern

😰 Find similar things on

Yahoo! image search

goodness!

Related tags:







From susancenics



From susancspics

Slideshow I







From Nicolas.

From ecwillet

From Larry Slinge







From Nicolas

© Li-Chiou Chen, Pace University

## Are there differences between the two pictures of a boat?



#### Metadata

- Data that describes other data
- Examples: author name, date and time of creation, company name, geolocation, etc.
- Does metadata reveals a part of your privacy?

### EXIF (Exchangeable Image File) format

- Commonly used to store digital pictures
- EXIF file stores metadata of the file
- Developed for storing metadata in JPEG and TIFF files
- With tools such as Exif Reader or online Exif extraction site, you can extract metadata from image file

#### Activity II: Metadata from a picture

### Go to Metapicz <u>http://metapicz.com/#landing</u>

- The picture of the boat with geolocation is
   csis.pace.edu/~lchen/pcap14/boat.jpg
- Enter the picture URL
- Take a look at the Exif information
- Where the picture was taken?

How is my web transactions secured?



#### How are the web transactions secured?

► https://www.facebook.com	🏠 ⊽ 🖱 🔀 र Google				
facebook	Email or Phone     Password       Log In       Keep me logged in     Forgot your password?				
Connect with friends and the world around you on Facebook.	<b>Sign Up</b> It's free and always will be. First Name				
See photos and updates from friends in News Feed.	Your Email Re-enter Email				
Share what's new in your life on your Timeline.	New Password				
<b>Find more</b> of what you're looking for with Graph Search.	Birthday Month Day Year Why do I need to provide my birthday? Female Male				
	By dicking Sign Up, you agree to our Terms and that you have read our Data Use Policy, including our Cookie Use.				

#### Activity III: Intercept/View Web Transactions

- We will use a web proxy software, Burp Suite, to cache and view your web transactions
- Download the software from <u>http://www.portswigger.net/burp/downloadfree.html</u>
- Save it on your computer desktop (it is a Java program)
- Double click on the program to run it.

#### Setting up Proxy

- Click on Proxy / Options
- Uncheck
  - □ intercept requests based on the following rules.
- Click on History tab to wait for web traffic

#### Setup Browser Proxy Configuration

- Open Firefox
- Tools/ Options / Advanced / Network /Settings
- Check
  - Manual Proxy Configuration
    - HTTP Proxy: 127.0.0.1 Port:8080
- Check
  - □ Use this proxy server for all protocols

#### Intercept and view web transactions

- In Firefox, browse <u>https://www.facebook.com</u>
- Type testing login information
- Login: test pass: test123
- On your proxy history tab, you should be able to see the transactions that are cached
- Find the one with the login credential
  On Burp, click on params

Burp Suite Free Edition v1.5	-											
urp Intruder Repeater Window He	lp											
Target Proxy Spider Scanner	Intruder R	Repeater	Sequencer	Decoder	Comparer	Options A	erts					
Site map Scope												
Iter: Hiding not found items: hiding CS	S. image and g	eneral bina	arv content:	hiding 4xx r	esponses: hic	dina empty fold	ers					
A https://developers.facebook.com	Host			Method			Params	Status	A Length	MIME type	Title	Comment
https://es-es.facebook.com	tos://es-es.facebook.com		anti-ment	OFT	UNL /			200	44077	UTIN	Welsome to Essehast	comment
https://es-la.facebook.com	nttps://w	ww.faceb	OOK.COM	GET	/			200	442/1	HIML	vvelcome to Facebook	
https://fbstatic-a.akamaihd.net	nttps://w	https://www.facebook.com https://www.facebook.com		PUST	/ajax/bz			200	050	script		
https://fr-fr.facebook.com	nttps://w			POST	/ajax/bz			200	856	script		
https://id-id.facebook.com	nttps://w	ww.faceb	OOK.COM	POST	/ajax/bz			200	856	script		
https://it-it.facebook.com	nttps://w	ww.faceb	ook.com	POST	/ajax/websto	orage/proce		200	4/8	script	-	
https://ko-kr.facebook.com	nttps://w	ww.faceb	IOOK.COM	PUSI	/iogin.pnp?io	gin_attempt=1		200	256/1	HIML	Гасероок	
https://m.facebook.com	nttps://w	ww.taceb	ook.com	GET	/about/priva	cy	0			HIML	,	
https://th-th.facebook.com	-											
https://vi-vn.facebook.com	Degues	Danna										
	Reques	si nespu	JIISC									
http://www.facebook.com	Raw POST req	Params uest to /log	Headers	Hex								
http://www.facebook.com	Raw POST requ Type	Params Uuest to /log	Headers	Hex			Val	lue				
http://www.facebook.com https://www.facebook.com	Raw POST requ Type URL	Params Uuest to /log	Headers	Hex Name login_atte	empt		Val 1	lue				
http://www.facebook.com	Raw POST requ Type URL Cookie	Params uest to /log	Headers	Hex Name login_atte datr	empt		Val 1 yy_	lue _mTlfOzM\	/iLSxyM_2hl2	Zfq		
http://www.facebook.com	Raw POST requ Type URL Cookie Cookie	Params uest to /log	Headers gin.php	Hex Name login_atte datr lu	empt		Val 1 yy_ RA	lue _mTlfOzM\ Eilqj-zMHxi	iLSxyM_2hl2 1Z9-NsSjhml	Zfq g		
http://www.facebook.com	Raw POST requ Type URL Cookie Cookie Cookie	Params Uuest to /log	Headers	Hex Name login_atte datr lu fr	empt		Val 1 yy_ RA 0vv	lue _mTlfOzM\ Eilqj-zMHx wVFGV4v	ʻiLSxyM_2hi2 iZ9-NsSjhml i87iJI7.AWXL	Zfq g Jv07ysGYD5KS	wJDJXOhl5ato.BTIK0G.pFM	y.AWWsHaP_
http://www.facebook.com	Raw POST requ Type URL Cookie Cookie Cookie Cookie	Params Uuest to /log	Headers j	Hex Name login_atte datr lu fr locale	empt		Val 1 yy_ RA 0vv en_	ue _mTlfOzM\ Eilqj-zMHx wVFGV4v _US	'iLSxyM_2hl2 hZ9-NsSjhml  87iJI7.AWXL	Zfq g Jv07ysGYD5KS	SwJDJXOhl5ato.BTIK0G.pFM	y.AWWsHaP_
http://www.facebook.com	Raw POST requ Type URL Cookie Cookie Cookie Cookie Cookie	Params Uuest to /log	Headers j	Hex Name login_atte datr lu fr locale reg_fb_gi	empt		Val 1 yy_ RAI 0vv en_ http	lue _mTlfOzM\ Eilqj-zMHxl wVFGV4vi _US ps://www.	iLSxyM_2hl2 hZ9-NsSjhml i87iJI7.AWXL facebook.co	Zfq g Jv07ysGYD5KS m/	SwJDJXOhl5ato.BTIK0G.pFM	y.AWWsHaP_
http://www.facebook.com	Raw POST requ Type URL Cookie Cookie Cookie Cookie Cookie	Params Uuest to /log	Headers j	Hex Name login_atte datr lu fr locale reg_fb_gr reg_fb_re	empt ate		Val 1 yy_ RAI 0vv en_ http http	Iue mTIfOzMV Eilqj-zMHxi wVFGV4vi US ss://www. ss://www.	iLSxyM_2hl2 IZ9-NSSjhmi 871J17.AWXL facebook.co facebook.co	Zfq g Jv07ysGYD5KS m/ m/	SwJDJXOhl5ato.BTIK0G.pFM	y.AWWsHaP_
http://www.facebook.com	Raw POST requ Type URL Cookie Cookie Cookie Cookie Cookie Cookie Cookie	Params Uuest to /log	Headers j	Hex Name login_atte datr lu fr locale reg_fb_ge reg_fb_re wd	empt ate ef		Val 1 yy_ RA 0vv en_ http http 123	ue _mTIfOzM\ Eliqj-2MHx WVFGV4v US JS://WWW. SS://WWW. 31x608	iLSxyM_2hl2 1Z9-NsSjhml 871J17.AWXL facebook.co facebook.co	Zfq g Jv07ysGYD5KS m/ m/	SwJDJXOhl5ato.BTIK0G.pFM	y.AWWsHaP_
http://www.facebook.com	Raw POST requ Type URL Cookie Cookie Cookie Cookie Cookie Cookie Cookie Cookie	Params Uuest to /log	Headers j	Hex Name login_atte datr lu fr locale reg_fb_ge reg_fb_re wd act	empt ate ef		Val 1 yy_ RA 0vv en_ http http 123 139	ue mTlfOzMV Eliqj-zMHx VVFGV4v US ss://www. 31x608 959341388	iLSxyM_2hl2 hZ9-NsSjhml 87UI7.AWXL facebook.co facebook.co 67/0	Zfq g Jv07ysGYD5KS m/ m/	SwJDJXOhl5ato.BTIK0G.pFM	y.AWWsHaP_
http://www.facebook.com	Raw POST requ Type URL Cookie Cookie Cookie Cookie Cookie Cookie Cookie Cookie Cookie Cookie	Params Uuest to /log	Headers j	Hex Name login_atte datr lu fr locale reg_fb_gi reg_fb_re wd act _e_0szi_	empt ate ef		Val 1 yy_ RA 0vv en_ http http 123 139 ["0e	Iue mTIfOzMV Eilqj-zMHx VFGV4vi US ss://www. ss://www. 31x608 959341388 szi <sup>2</sup> ,13959	iLSxyM_2hi2 hZ9-NsSjhml 87UI7.AWXL facebook.co facebook.co 67/0 34138871,"a	Zfq g Jv07ysGYD5KS m/ m/ ct",1395934138	SwJDJXOhl5ato.BTIK0G.pFMy 867,0,"pass","click","click","blu	y.AWWsHaP_ ebar","r","/",{"ft":{
http://www.facebook.com	Raw POST requ Type URL Cookie Cookie Cookie Cookie Cookie Cookie Cookie Cookie Cookie Cookie Cookie Cookie Cookie	Params Uuest to /log	Headers j	Hex Name login_atte datr lu fr locale reg_fb_gi reg_fb_re wd act _e_0szi_ lsd	empt ate ef		Val 1 yy_ RA 0vv en_ http 123 135 ["0: 0v0	Iue mTIfO2MV Eilqj-2MHx VFGV4vi US ss://www. ss://www. 31x608 959341388 szi*,13959	iLSxyM_2hi2 hZ9-NsSjhml 87UI7.AWXL facebook.co facebook.co 67/0 34138871,"au	Zfq g Jv07ysGYD5KS m/ m/ ct",1395934138	SwJDJXOhl5ato.BTIK0G.pFMy 867,0,"pass","click","click","blu	y.AWWsHaP_ ebar","r","/",{"ft":{
http://www.facebook.com	Raw POST requ URL Cookie Cooki	Params Uuest to /log	Headers j	Hex Name login_atte datr lu fr locale reg_fb_gi reg_fb_re wd act _e_0szi_ lsd email	empt ate ef		Val 1 yy_ RA 0vv en_ http 123 135 ["0s AM	Iue mTIfOzMV Eilqi-zMHx VFGV4vi US ss://www. ss://www. 31x608 959341388 959341388 szī*,13959 ipb959 –	iLSxyM_2hiZ nZ9-NsSjhml 87UI7.AWXL facebook.co facebook.co 67/0 34138871,"a	Zfq g Jv07ysGYD5KS m/ m/ ct",1395934138	SwJDJXOhl5ato.BTIK0G.pFMy 867,0,"pass","click","click","blu	y.AWWsHaP_ ebar","r","/",{"ft":{
http://www.facebook.com	Raw POST requ URL Cookie Cooki	Params Uuest to /log	Headers j	Hex Name login_atte datr lu fr locale reg_fb_gi reg_fb_re wd act _e_0szi_l lsd email pass	empt ate ef		Val 1 yy_ RAV 0vv en_ http http 123 135 ["0: AV tess tess	Iue mTIfO2MV Eilqj-2MHx VFGV4vi US ss://www. 31x608 959341388 szi*,13959 st t123	iLSxyM_2hi2 hZ9-NsSjhml 87UI7.AWXL facebook.co facebook.co 67/0 34138871,"a	Zfq g Jv07ysGYD5KS m/ m/ ct",1395934138	SwJDJXOhl5ato.BTIK0G.pFMy 867,0,"pass","click","click","blu	y.AWWsHaP_ ebar","r","/",{"ft":{
http://www.facebook.com	Raw POST requ URL Cookie Cooki	Params Uuest to /log	Headers j	Hex Name login_atte datr lu fr locale reg_fb_gr reg_fb_re wd act _e_0szi_ lsd email pass default_p	empt ate ef 0		Val 1 yy_ RAA 0vv en_ http http 123 139 ["0s AM tes tes	Iue mTIfO2MV Eilqj-2MHx WFGV4vi US ss://www. ss://www. 31x608 959341388 szi*,13959 st t123	fiLSxyM_2hi2 hZ9-NsSjhml 87UI7.AWXU facebook.co facebook.co 67/0 84138871,"a	Zfq g Jv07ysGYD5KS m/ m/ ct",1395934138	SwJDJXOhl5ato.BTIK0G.pFMy 867,0,"pass","click","click","blu	y.AWWsHaP_ ebar","r","/",{"ft":{
http://www.facebook.com	Raw POST requ URL Cookie Cooki	Params Uuest to /log	Headers j	Hex Name login_atte datr lu fr locale reg_fb_gi reg_fb_re wd act _e_0szi_ lsd email pass default_p timezone	empt ate ef 0 bersistent		Val 1 yy_ RAA 0vv en_ http 123 139 ["0s 440 test test 0 240	Iue mTIfOzIMV Eilqi-zIMHX wVFGV4vi US uS s://www. s://www. 31x608 959341388 szi*,13959 st t123	iLSxyM_2hi2 hZ9-NsSjhml 87JJ7.AWXL facebook.co facebook.co 67/0 34138871,"a	Zfq 9 Jv07ysGYD5KS m/ m/ ct",1395934138	SwJDJXOhl5ato.BTIK0G.pFM 867,0,"pass","click","click","blu	y.AWWsHaP_ ebar","r","/",{"ft":{
http://www.facebook.com	Raw POST requ URL Cookie Cooki	Params Uuest to /log	Headers j	Hex Name login_atte datr lu fr locale reg_fb_gi reg_fb_re wd act _e_0szi_l lsd email pass default_p timezone lgnrnd	empt ate ef 0 wersistent		Val 1 yy_ RAA 0vv en_ http 123 133 ["0s 434 tes 0 240 082	Iue mTIfOzIMV Eilqj-zIMHX wVFGV4vi US US S://www.	fiLSxyM_2hiZ hZ9-NsSjhml 187JJI7.AWXL facebook.co facebook.co 67/0 34138871,"a	Zfq 9 Jv07ysGYD5KS m/ m/ ct",1395934138	SwJDJXOhl5ato.BTIK0G.pFMy 867,0,"pass","click","click","blu	y.AWWsHaP_ ebar","r","/",{"ft":{
http://www.facebook.com	Raw POST requ URL Cookie Cooki	Params Uuest to /log	Headers j	Hex Name login_atte datr lu fr locale reg_fb_gi reg_fb_re wd act _e_0szi_l lsd email pass default_p timezone lgnrnd lgnjs	empt ate ef 0 versistent		Val 1 yy_ RAA 0vv en_ http 123 135 ["0: 430 tes tes 0 240 082 139	Iue mTIfOzIMV Eilqj-zIMHX wVFGV4vi US US S://www.	fiLSxyM_2hiZ hZ9-NsSjhml 187JJI7.AWXL facebook.co facebook.co 67/0 34138871,"a 1	Zfq 9 Jv07ysGYD5KS m/ m/ ct",1395934138	SwJDJXOhl5ato.BTIK0G.pFM 867,0,"pass","click","click","blu	y.AWWsHaP_ iebar","r","/",{"ft":{}

#### Clean Up

• Click exit to close Burp Suite when you are done.

Open Firefox

- Tools/ Options / Advanced / Network /Settings
- Check
  - No Proxy
- Click OK

#### Man in the Middle



#### **Resources: Watch Video**

DoD DISA video on cybersecurity awareness

http://iase.disa.mil/eta

#### PCAP summer research opportunity

#### The Project

- Investigate the use of social networking messages, such as Facebook posts, to authenticate authors
- Collect data from social networking sites
- □ Identify stylometry or other features in these messages
- Use machine learning algorithm (Support Vector Machine)
- □ Current accuracy rate from our study: 85% on average
- Download and fill up the application form
   csis.pace.edu/~lchen/pcap14/

#### **Questions / Comments**

