Securing Information in a Mobile World

Thu, Jan 21 | 2:00 p.m. – 3:30 p.m.

PRESENTED BY:
Charlie LeBlanc, William Figures, and Blad Slavens
A Brief History of Computing and Software for Schedulers and Dispatchers

Systems in the 80’s and early 90’s were computer-centric and pretty secure…. Why ??????
And then came the Internet !!!!
Highly technical description of the Internet

“The Internet is a data network that connects “everything” together” (kind of like the phone system !) - William Figures 2007
The ‘Net(work) as a computing platform: Using WEB Services

WEB SERVICES=FARS
Is it safe to use public Wi-Fi?
Security challenges when using public Wi-Fi

Some things to know about public Wi-Fi hotspots

- Unlike your home Wi-Fi access point, most public Wi-Fi hotspots at hotels, restaurants, coffee shops, airports, etc. do not use encrypted communication.
- This means that all your data may be sent in clear-text across the wireless network. Anyone with a “sniffer” could then snoop on your connection.
- In order to secure their Wi-Fi properly, a business owner would have to issue a password to connect to the hotspot. To be truly secure, this password would be unique to a single person.
- Since this isn’t feasible, you need to take other precautions to secure your data when using a public hotspot.

Sources:
Case Study: Firesheep browser extension

Coder exposed risk to Facebook users at public hotspots

- To call attention to glaring security vulnerabilities with both Facebook – and other sites – and public Wi-Fi, a “white hat” hacker developed a Firefox extension that allowed a user to hijack the Facebook account of anyone logged into the same Wi-Fi hotspot.
- Facebook used encryption while logging in but not for the cookie created by the login.
- Most sites patched the security flaw, but the underlying Wi-Fi issue remains.

Sources: [https://en.wikipedia.org/wiki/Firesheep](https://en.wikipedia.org/wiki/Firesheep)  
1. Make sure you use secure websites (https)

Always looks for https:// + lock icon in the Address bar.

- Don’t enter any sensitive data, e.g. usernames, passwords, credit card info, ID numbers, account numbers, etc., unless you see the https prefix in the address bar of your browser, ex.: https://www.google.com.
- Most current browsers also show a lock icon next to the address. The icon should be in the locked position.
- If you see an unlocked icon or a lock with a warning message, or don’t see a lock at all, don’t enter sensitive data into that site.

Sources:
https://commons.wikimedia.org
2. Install HTTPS Everywhere in your browser.

Ensures you’ll always get secure versions of webpages.

- HTTPS Everywhere is a browser extension designed to choose the secure version of websites and web pages.
- Saves you from having to always type in “https://” for every web address.
- Doesn’t work on sites which don’t support https at all; only works on sites that support it but may not link to the secure versions by default.

Sources:
https://www.eff.org/https-everywhere/faq
3. Use a Virtual Private Network (VPN)

VPNs are not just for connecting to the office network.

- Anyone can use a VPN. It’s not limited to workplaces.
- When using a VPN, all your data is encrypted once it leaves your computer.
- Many VPN services but almost all have a monthly fee.

Sources:
http://www.pcmag.com/article2/0,2817,2419611,00.asp
4. Turn your phone into a Wi-Fi hotspot

Your phone can be used instead of the public hotspot.

- Your smartphone should have a setting called “Mobile Hotspot.”
- This creates a secure password-protected, encrypted Wi-Fi connection that you can then use for your other devices.
- Be aware of your data charges though, particularly if traveling overseas!

Sources:
5. Turn off file sharing

Your computer may share your files by default.

Windows and Mac OS X have an option to share files across a network, including a Wi-Fi network. It may be on by default, so disable it.

Sources:
http://windows.microsoft.com/en-US/windows-8/turn-sharing-on-or-off
http://www.udel.edu/topics/virus/security/mac/macsecure.html
Data security for Flight Department Data

What are our goals/requirements for the state of our data
Data security for Flight Department Data

Types of data stored in Flight Department management systems

• Aircraft movement (both future and historical)

• Passenger movement (both future and historical)

• Personally Identifiable Data (PII or PID) for Passengers, Crew, other personnel
Value of the Data to the Company Flight Operation

1. Maintaining data to increase communication between department personnel and customers

2. Historical data used to ensure (government and corporate) compliance as well as planning for future needs
Value of the Data to “Outsiders”

Who wants my data anyway ??????

• Competitors
• Foreign entities
• Bad guys (terrorists ??)
• Hackers
How does Sensitive Data “Leak” Out of the System

• System intrusions

  • Internal system intrusions

Competition within your corporate structure could make the flight department data a target for an internal attack.

One of the best known intrusion methods are login and password data posted at a user's desk.
How does Sensitive Data “Leak” Out of the System

• System intrusions

  • External Intrusions

    Susceptible to social engineering.

Portable device access opens a whole range of exposure to external attacks
How does Sensitive Data “Leak” Out of the System

• Social engineering

  • Multi levels of social engineering are constantly evolving

  • Limited only to the ingenuity of the “hacker” and the unawareness of the “target”

Fix - **BE AWARE** !!!!!!
How does Sensitive Data “Leak” Out of the System

• Unencrypted communications across the public Internet

  • Including

    • EMAIL – plain text email and unencrypted attachments
      Alternative methods of sending information

    • General unencrypted data transmissions (web sites)
      What does that https:// thingy mean anyway
How does Sensitive Data “Leak” Out of the System

• Data mismanagement by employees, vendors and ancillary personnel
The Internet’s dirty little secret !!!!
The ‘Net(work) as a computing platform - Using WEB Services

WEB SERVICES = FARS
F = Fast
A = Accessible
R = Reliable
S = Secure
How Email Works

I do not like that Sam-I-am!
Do you like green eggs and ham?
I do not like them, Sam-I-am.
I do not like green eggs and ham

Email servers exchange data !!!

Sam

Pam
Internet connections
Typical Internet Router Trace

Visual Trace Route Tool

approximate geophysical trace

trace the path to a network

Remote Address: www.usairways.com

Host Trace: yougetsignal.com

Proxy Trace:

trace information

Proxy trace to www.usairways.com
27 hops / 19.2 seconds

1. Unknown
2. myvzw.com
3. myvzw.com
4. myvzw.com
5. alter.net
6. ALTER.NET
7. ALTER.NET
8. ALTER.NET
9. ALTER.NET
10. niayer.net
11. niayer.net
12. niayer.net
13. niayer.net
14. 192.241.192.253
15. niayer.net
16. niayer.net
17. niayer.net
18. niayer.net
19. ntt.net
20. 192.205.37.57
21. att.net
22. att.net
23. att.net
24. att.net
25. 12.127.141.38
26. 12.47.204.125
27. 12.47.204.75

~2,993 miles traveled
How Email Works

I do not like that Sam-I-am!
Do you like green eggs and ham?
I do not like them, Sam-I-am.
I do not like green eggs and ham
How Email Works
Got their password. I can sell this on the Internet. Lobster for dinner tonight !!!

Kneivel
Do you Really Want to Send this Email ????

DATE: Mon. 01/13/2014  PAX MANIFEST - TAIL# N1PFM  JET (12 seats) PAGE 3

TRIP COMMENT: Printout @ 01-13/11:04

HAMMER, MICHAEL
DEPT: ACCT: S0093 FLIGHT STATUS: AUTH:
OFFICE: HOME: 555 E CITY AVE Bala Cynwyd, PA 19004
PHONE: 913-245-6167 PHONE: 484-562-0047 PHONE:
CITIZENSHIP# PASSPORT# DOB: 05/22/1980 CHARGE: -- DRIVER APP'L:
COMMENTS: US40219-ee-2323 EXP: 11/22/2015
NOTES:

HARRIS, DONALD
DEPT: ACCT: S0031 FLIGHT STATUS:
OFFICE: HOME: PRENT:
PHONE: PRINT:
CITIZENSHIP# PASSPORT# DOB:
COMMENTS:
NOTES:

See more about steve.jones@my.europen_handler.com.
Taking Responsibility for Ensuring Data Security and Integrity

• Your role in maintaining data security (is it my job ???)

It needs to be everyone’s job. Having access to sensitive data implies the responsibility to care for it. Don’t blame IT if you hit the “SEND” button without thinking about it.
Maximizing data security in an ever-changing hostile environment means minimizing the risks.

Threats to data security are constantly evolving. Your organization needs to keep up with current trends. Your IT department and/or supporting vendors have an obligation to keep your department up to date re: the latest security best practices. It is important to listen to what they have to say.
Taking Responsibility for Ensuring Data Security and Integrity

- Your organization needs to support constant vigilance.
- Take the responsibility to make sure that security procedures are maintained.
- Once a data security policy is in place, make sure it is adhered to by all employees.
Designing information dissemination on a need to know basis.

Don’t just send a document outside of your organization because it contains info needed by an outside service. Make sure that documents are designed to relay only pertinent information. Extraneous information could fall into the wrong hands.

Developing secure methods for dissemination of flight operations data.

Make sure that accepted data encryption policies and procedures are in force anytime you are send any type of PII.
How should I secure my passwords?
Possible password combinations

- lc
- lc + UC
- lc + UC + 123
- lc + UC + 123 + $#%&
Password Security

These tips will help you when setting passwords

• Use strong passwords: mix upper- and lowercase, numbers, characters.
• Use a different password unique to each important website.
• Use two-factor authentication when available.
• Use a password manager.

Sources:
https://www.google.com/goodtoknow/online-safety/passwords/
Case Study: LinkedIn.com password breach

2012 LinkedIn hack exposed users’ passwords

• In June 2012, Russian hacker(s) stole passwords of 6.5 million LinkedIn users and then posted them on the internet
• LinkedIn used poor encryption practices, i.e. encryption without using a “salt”, allowing the hackers to “crack the code”
• Some popular passwords: 1234, linkedin, letmein, password, ihatemyjob
• Hacker didn’t post usernames or e-mail addresses, though theoretically they were in possession of them

Sources:
http://mashable.com/2012/06/06/6-5-million-linkedin-passwords/#uAG4t_XfGuqW
https://en.wikipedia.org/wiki/2012_LinkedIn_hack
1. Use strong passwords: mix upper- and lowercase, numbers, characters.

<table>
<thead>
<tr>
<th>Characters Used</th>
<th># of Characters</th>
<th>Password Length</th>
<th># of Possible Password Combinations</th>
</tr>
</thead>
<tbody>
<tr>
<td>lc</td>
<td>26</td>
<td>8</td>
<td>208,827,064,576 (208 billion)</td>
</tr>
<tr>
<td>lc + UC</td>
<td>52</td>
<td>8</td>
<td>53,459,728,531,456 (53 trillion)</td>
</tr>
<tr>
<td>lc + UC + 123</td>
<td>62</td>
<td>8</td>
<td>218,340,105,584,896 (218 trillion)</td>
</tr>
<tr>
<td>lc + UC + 123 + $%#^</td>
<td>95</td>
<td>8</td>
<td>6,634,204,312,890,620 (6 quadrillion)</td>
</tr>
</tbody>
</table>
Creating strong passwords

If a hacker can hack 1,000,000 passwords per second…

and your 8 character password uses:

lowercase letters only

Your password can be cracked in ~ 29 hours
Creating strong passwords

If a hacker can hack 1,000,000 passwords per second…

and your 8 character password uses:

lowercase + UPPERCASE

Your password can be cracked in ~ 11 months
Creating strong passwords

If a hacker can hack 1,000,000 passwords per second…

and your 8 character password uses:

lowercase + UPPERCASE + digits 0-9

Your password can be cracked in ~ 3 years
Creating strong passwords

If a hacker can hack 1,000,000 passwords per second...

and your 8 character password uses:

lowercase + UPPERCASE + digits 0-9 + special keyboard characters

Your password can be cracked in ~ 105 years
2. Use a different password for each website

If your account is hacked at one, then it could expose others.

• Never reuse your password for a sensitive or crucial site on another site.
• These sites are the most crucial and should be protected by unique passwords:
  – Banking / Credit Card accounts
  – E-mail accounts
  – Social Media accounts
  – Other sites containing financial information (tax prep, credit bureau, Mint.com, etc.)

Sources:
https://security.illinois.edu/content/why-you-should-use-different-passwords
https://nakedsecurity.sophos.com/2013/04/23/users-same-password-most-websites/
3. Use two-factor authentication if available

2FA adds another layer of protection to passwords

- Two-factor authentication (2FA) is based on possessing two things simultaneously:
  - Something you know (PIN, password, answer to a security question, etc.)
  - Something you have or something you are (password token, smartphone, mag stripe card, biometrics)
- Both must be used to authenticate you.
- You already use 2FA today. Example: ATM card + PIN
- Two types of 2FA: every time you login or first time logging in to a new device
- Most common 2FA implementation is sending an SMS message with a 2nd code

https://en.wikipedia.org/wiki/Two-factor_authentication
4. Use a password manager

A password manager has many features to help protect your accounts

- Can generate good passwords for you.
- Always encrypts your passwords when storing them.
- In some cases can synchronize across devices.
- Allows you to secure all of your passwords with one very secure one.
- Sometimes can be set up to use 2FA.

Sources:
http://www.pcmag.com/article2/0,2817,2407168,00.asp
Some popular password managers

Here are some password managers to consider

Sources:
http://www.pcmag.com/article2/0,2817,2407168,00.asp
http://lifehacker.com/5529133/five-best-password-managers
Flight Departments and Social Media

• Operating in the digital age.

• Myriad of outlets – Not just Facebook and Twitter

Source: http://www.flashdancersnyc.com
Flight Departments and Social Media

- Posting about where you work.
- Letting people know what you do.
  - Pilot? Flight Scheduler? Security Manager?

John Kimble
Just landed a job flying for XYZ’s corporate aviation department. I am very excited to travel the world!
Like · Comment... · 9 minutes ago ·

4 people like this.
Congratulations! Keep us posted on where you fly.
Flight Departments and Social Media

• Operating in the digital age.

• Telling the world how you feel about what you do.
  – Disgruntled employee could be easily compromised.

 wow sometimes I just don’t know about this job. #stressed #horribleboss

  – May establish pattern of travel for VIPs.

 03:35 AM - 20 Jan 13 · Embed this Tweet
Posting to Social Media

- Sending out a tweet, posting a Facebook status

- “Heading to Paris. I love this city. #workinghard”- hashtag gives away that the trip is professional, not personal.

- Threats to physical security
- Raises questions about business. Why is CEO in Paris?

- Criminal organizations or competing businesses set up a fake twitter account posing as a pilot, security manager, crew chief etc…
- Fake twitter profile could engage the employee, ask questions.
- Fake recruiting
Posting to Social Media

- Sending out a tweet, posting a Facebook status
- Posting information to friends’ wall believing it is private. They comment or otherwise cross-post it, opening it to the public.
- Criminal organizations or competing businesses can set up a fake twitter account posing as a pilot, security manager, crew chief etc…
- Fake twitter profile could engage the employee, ask questions.
- Fake recruiting

Source: www.itconflict.com
Corporate Espionage

- Digital Honey Traps, Disgruntled Employees

- Recent trend of people being “catfished”, lured into a fake relationship by a hostile party posing as an attractive woman.

- This could easily happen to a flight department employee, especially if they make it clear through social media they are lonely, recently divorced etc…

- Disgruntled employees are easily compromised. Signs of frustration often posted to social media.

  Ben Richards
  I hate my job, my GF just left me last week and now my car battery is dead. What else could go wrong? Sorry just needed to vent.
  Like · Comment · Yesterday · 😞

  [2 people like this.]

  Keep your head up mate. Life has a way of working itself out.
Social Media and Location Security

- Broadcasting locations, dates and times.

- Gives potential kidnappers vital information
  - Names of the people
  - Names of city (Cancun) and the nightclub (Mandala)

- Facilitates virtual kidnapping.

“#cancun #mandala #muybuena
@gabrielherrerad @fernandodelagarza
@maurogarza by diegotrevin”

-from Twitter/Instagram on 12 April 2013

- [http://richkidsofinstagram.tumblr.com](http://richkidsofinstagram.tumblr.com)
Social Media and Location Security

• Source: MSNBC via the Associated Press/Francois Mori
How do I protect my mobile device?
1. Encrypt your mobile disk drives

Fully encrypting a file storage device renders it unreadable without the password or backup key.

Without encryption, someone can connect your drive to another machine and read its entire contents.

Sources: https://technet.microsoft.com/en-us/library/cc731549%28v=ws.10%29.aspx
https://support.apple.com/en-us/HT204837
Full Disk Encryption:

Some things to know about encrypting portable disks…

- All laptop drives and USB-type drives, e.g. flash/thumb drives and portable hard drives, need to be encrypted.
- Contents of the disk drive cannot be read until the password is entered that unlocks the data.
- If you forget the password or lose the backup key, contents are useless – even to you!
- Must enter the password each and every time the device powers on. But once on, the contents of the drive will continue to decrypt automatically.

Sources:

http://whatis.techtarget.com/definition/full-disk-encryption-FDE
Encryption software options

- **BitLocker**
  - Built-in encryption tool for Windows machines
  - Available in premium versions of Windows

- **FileVault**
  - Built-in encryption tool for Mac machines
  - Available in all versions of OS X

- **VeraCrypt**
  - Open source encryption built on defunct TrueCrypt
  - Available for Windows/Mac/Linux

**Sources:**
- [https://veracrypt.codeplex.com/](https://veracrypt.codeplex.com/)
Partial Disk Encryption: an alternative

Keep these concerns in mind if choosing partial disk encryption instead of full-disk encryption.

- With Partial Disk Encryption, only a part of the drive is encrypted, and you can put your sensitive documents there.
- Pro: Machine isn’t rendered completely useless if you forget the key.
- Con: Not as secure. Often contents of your sensitive documents may reside unknowingly on the unencrypted sector of your hard drive. Example: MS Office auto-save files.

Sources:
http://www.pcworld.com/article/148513/article.html
2. Keep a copy of your computer serial #s

Having your serial number will help recover a lost device

Some places to find your serial #:

- Tag on the machine or device.
- System settings or “About …” menu
- Receipt or packing slip from when you purchased it

Your chances of recovery are much greater when you can positively identify your device

Sources:

http://ramcomputers.apps.uri.edu/help
3. Backup your data!

You’ll lose data at some point in your life. So back it up!

- Follow the 3-2-1 Rule for backing up data:
  - File 3 copies of all important data (original + 2 copies)
  - Stored on 2 different media (ex. DropBox + DVD, SD card + portable HD)
  - Keeping 1 backup offsite. (ex. office, cloud-based storage, safe deposit box)

- There are many seamless and/or online backup options today: Carbonite, DropBox, Google Drive, iCloud, Time Machine

Sources:
http://blog.trendmicro.com/trendlabs-security-intelligence/world-backup-day-the-3-2-1-rule/
http://lifehacker.com/5961216/why-you-should-have-more-than-one-backup
What do I do if my mobile device is lost or stolen?
1. If you are unharmed, don’t go to the police .... yet!

- If you are physically safe, your first priority should be to protect your data and identity.
- There will be time to file a police report soon enough.
2. Start changing your passwords immediately!

Passwords are the keys to your data. Protect them.

- Find a computer as quickly as possible. If your only computer was stolen, find a friend’s, family member’s or a workplace computer.

- Begin by changing your critical passwords in this order:
  1. E-mail (This is the key to all other passwords, i.e. “Forgot my password” messages)
  2. Financial institutions (banks, credit card companies, etc.)
  3. Social media accounts (Facebook, Twitter, LinkedIn, etc.)
  4. Everything else

- If you use a password manager, then it can help you reset those passwords.
3. Remote wipe your device.

Nearly every recent version of any smartphone OS allows a user to wipe a phone from a remote location.

- If you have reason to believe that your device fell into the wrong hands, i.e. stolen or irretrievably lost, then you should wipe your device clean.
- Remote wiping a phone returns it to its original factory settings.
- The device will be erased the next time it attempts to connect to the cellular network.
How to remote wipe your device

**iPhone / iPad**
- Login to iCloud.
- Find the device.
- “Erase.”

**Android**
- Login to Android Device Manager.
- Find your phone.
- “Remote Wipe.”

**Windows Phone**
- Login to WindowsPhone.com.
- “Find My Phone.”
- “Erase.”

Sources:
[https://support.google.com/a/answer/173390?hl=en](https://support.google.com/a/answer/173390?hl=en)
4. Try to track your lost device.

- Keep in mind, remote wiping your device will usually render tracking useless. So you usually have a choice to make: wipe or track?
- You don’t necessarily have to have installed a tracking app before the phone is lost.
- NEVER attempt to retrieve a device from a thief yourself. Leave that job to the police.

Sources: http://www.digitaltrends.com/mobile/how-to-track-a-cell-phone/2/
http://www.digitaltrends.com/computing/can-location-tracking-services-help-recover-your-stolen-smartphone-tablet-or-notebook/
5. Report your lost phone to your carrier.

- Some carriers may offer protection against unauthorized charges, if the phone is reported as lost or stolen in a timely manner.
- A lost or stolen phone can be reported by calling your carrier’s customer support. You may be able to file the report online for some carriers.
- Once the cellular service is suspended, it may make it difficult or impossible to track or wipe the phone.
- Carrier may require a police report if you are attempting to replace the device.

Sources:
http://how-to.t-mobile.com/lost-or-stolen-phone/
https://www.fcc.gov/stolen-phones-contact-numbers
6. File a police report.

May be necessary for insurance or replacement service.

Reasons to file a police report:
• May be required by your insurance company or your employer.
• Helps the jurisdiction keep accurate crime statistics.

Reasons not to file a police report:
• Can take a lot of time and not likely to yield fruitful results. Police departments are overburdened and have other more pressing concerns.
• In developing regions, police corruption may be a concern. Consult with your corporate security or with a trusted local for advice.

Sources:
7. Sign-up for credit monitoring service

Credit monitoring will alert you if someone opens an account in your name.

- Service can send you an e-mail or text message if any new activity is detected.
- Doesn’t prevent an account from being opened.
- May qualify for free service from retailer, a bank, or from an organization like AAA.
- Consumer Reports doesn’t think it’s worth it unless it’s free.

Sources: [http://www.consumerreports.org/cro/magazine/2013/01/don-t-get-taken-guarding-your-id/index.htm](http://www.consumerreports.org/cro/magazine/2013/01/don-t-get-taken-guarding-your-id/index.htm)
8. Put a lock on or freeze your credit

A credit report “lock” or “freeze” means that lenders can’t access your report to approve new lines of credit or open new accounts.

Sources: TransUnion.com, Equifax.com, Experian.com major credit bureaus
Credit Report Lock or Freezes:

Some things to know about credit report locks

- prevent banks and others from accessing your credit report, meaning they won’t open a new credit account to anyone – including you!
- can be temporarily or permanently lifted, and in some cases, unlocked only for certain parties.
- won’t lower your credit score.
- in some states, may be provided free of charge for identity theft victims.
- can be done online or by calling the credit bureau.

Sources:
http://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs
Data Security Overseas

High Cyber Threat Locations – Government Based

Know the risks (email / document compromised)
Know the places (China, Russia, E. Europe)
Know the tactics (Hotel rooms)
Know your policies (personal vs. work devices)
DEDICATED TO HELPING BUSINESS ACHIEVE ITS HIGHEST GOALS.