

Preparing your digital assets for traveling the world





Jack Daniel, CCSK, CISSP, MS MVP Enterprise Security

Product Manager, Tenable Network Security





You need a plan

That means you need to ask some questions first:

- What *can* I take?
- What do I *need* to take?
- What do I *want* to take?

And more questions:

- Where am I going?
- What happens if I lose my stuff?
- What sensitive resources am I exposing?
(This is trickier than it sounds)
 - No documents + VPN credentials = a lot of documents



Paranoia level?

I don't care, I don't have to.

Besides, what could possibly go wrong?

Of course I'm taking all that stuff, why not?

Travel overseas?

Are you nuts?

Other countries are full of foreigners and other criminals.



Warning:
the following slides are
full of words



General guidelines:

- Never use systems other than your own for anything but completely public info
- Maintain physical control of your stuff
- Do not trust hotel safes
- Use shielded passport sleeves and wallets
- US credit and debit cards often do not work in modern countries
 - No chip and pin
- Label your stuff
- Tell CC companies and banks about ~~overseas~~ *any* travel



General hardware guidelines

- Do not use USB charging stations
- If you can, always keep your hard drive with you
- Do NOT have a password manager installed on any device you carry, it is a single point of compromise
 - I like them in most environments
- Remove batteries when not in use
 - Prevents quick booting and rooting
 - Saves battery life
- ALWAYS fully power down/hibernate, do not sleep, do not trust “locked”



Devices

- Phones
- Laptops, tablets
- Cameras, camcorders, Audio recorders
- Tablets
- PDAs (anyone still use one?)
- GPS?

Removable media

- Flash drives
- CF/SD cards
- CDs/DVDs
 - Including the ones *in* your gear



There are no trusted networks



VPNs

- Plural for a reason:
 - PPTP, insecure and unreliable
 - L2TP/IPsec (NOT plain L2TP), more secure, still flaky
 - Traditional IPsec, secure and fairly reliable
 - SSL: multiple types
 - *In-browser, true clientless: convenient, but potentially horrible*
 - *In-browser with scripted client: probably better, but have issues*
 - *Installed SSL client: probably secure, may be flexible*
 - *OpenVPN allows choice of port and protocol*



VPNs, continued

- You want multiples available, on different ports and protocols
 - *TCP 443 is likely to be open, but may be proxied.*
 - *UDP 53 may be open, also may be proxied/blocked.*
- I usually have at least two servers listening
- Don't forget:
 - SSH
 - Commercial services
 - TOR



VPNs, continued

- VPN clients on phones, tablets, laptops, etc.
- Restrict what can be accessed by the VPN!
- Ideally different VPNs depending on sensitivity
 - Full tunnel for privacy and security
 - Split for access to resources.



Data:

- Don't take it
- Don't access it
- If you take it, encrypt it
 - But know you WILL give up the keys
 - Maybe nested crypto
- Better: encrypt and store online.
 - SkyDrive, Wuala, dropbox*, etc.
- Take as little as possible
 - This means scrubbing your stuff if you don't use dedicated hardware
- Think about contact lists and other “incidental” information



Data:

- Consider a “disposable” webmail account
 - NOT Yahoo. Ever. Not Hushmail, either
 - For very different reasons
 - Store public info and “safe” contacts
 - *Maps, schedules, tourist info, etc.*
 - Maybe some encrypted files
 - Use unique username pattern, use unique, long passphrase



Data:

- Crypto: use what you know. Lacking that, use TrueCrypt
 - Bitlocker, MS Office, many others are decent, too
 - IF you use a decent passphrase



Extreme:

- Take nothing, access nothing.
- If needed, purchase disposable computer, phone, and regional SIM card
 - Before leaving, or in country
 - Pay cash, small bills, local currency
 - Never use for sensitive or private communications or storage.



Less Extreme:

- If needed, purchase disposable computer, phone, and regional SIM card
 - Before leaving, or in country
 - Don't use for sensitive or private communications or storage.
- Wipe and reload computer before and after each trip.
 - Or wipe and donate after trip.



Practical, if imperfect:

- Buy a spare hard drive, (preferably SSD), perform a clean install, leave main HDD at home.
 - Don't use for sensitive or private communications or storage.
- Wipe and reload travel HDD *immediately after* each trip.
 - A clean disk image can really speed things up here.
- Alternately, remove HDD, run off of bootable media (CD/DVD/SD/USB)
 - Probably only viable for Linux users.



Not so extreme:

- Initiate and answer all calls with warning/disclaimer, use similar if you use email:
 - “I am overseas, assume this message is being intercepted by hostile parties”
 - “Hostile parties” may mean
 - *Governments*
 - Ours
 - Theirs
 - Other
 - *Criminal or terrorist organizations*
 - *Commercial organizations*



Laptop hardening

- Update, update, update
- Firewall installed and on
- Anti-malware up to date
 - And set to manually update, not automatically
- Disable all auto-updates while you are at it
- Secunia PSI
- Bluetooth OFF
- Wireless off by default
- Vulnerability scan and remediate
- Follow hardening guides

Paradox:

- Crappy internet access means you have to take things with you
- Bringing data is insecure





Shameless Self Promotion:

My Blog:

blog.uncommonsensecurity.com/

Pauldotcom Security Weekly Podcast:

pauldotcom.com/

Tenable Network Security Podcast

blog.tenablesecurity.com/podcast/

And, of course, Twitter

twitter.com/jack_daniel