Travel Security

Ryan Lackey <ryan@venona.com>
B8B8 3D95 F940 9760 C64B DE90 07AD BE07 D2E0 301F
@octal

BalCCon 2k17 - Novi Sad, Serbia - 17 September 2017

Overview

- System to think about relative risk of travel
- Tactics, Techniques, Procedures for safer travel
- Examples of things which worked and didn’t
- Future research/development opportunities
- **Now with 100% more Donald Trump!**

Who am I?

- Cypherpunk from the early 1990s
- HavenCo: offshore datahaven in the North Sea
- Iraq/Afghanistan for ~8 years
- Trusted Computing startup (CryptoSeal)
- Network security vendor (Cloudflare)
- Now: startup making secure computing devices

More important cred!

- Traveled to >100 countries* worldwide
- Frequent work and personal travel
- Frequent traveler in multiple programs
- Interested in quasi-safe/adventure destinations
- Nerd; lots of computer gear when I travel
- Probably on several “lists”

Why is travel special?

- Exposure to multiple jurisdictions
- Weaker/special laws around borders and search
- Away from support
- Out of your ordinary experience
- High value population for targeting
- Always changing/evolving threats

Why do we care now?

- Always has been a concern for governments/IC
- New: Rise of economic espionage
- New: Many countries being more aggressive due to terrorism and security concerns
- New: Volume of routine international travel high
- New: People travel with very connected devices

Traits of risky travel

- International
- Initiated by someone other than you
- Schedule known to attacker in advance
- Unusual for you, but also routine can be risky

Who are high-risk travelers?

- Some people on their own (“Zero to Snowden”)
- Employment or associates as targets
- Source countries, transit, destination
- History of being a target

Hard problem

- Standard security problems with no silver bullet
- Lots more variables; even harder to generalize
- Rather challenging users (senior/independent)
- Balance of productivity vs. security already hard
- Constant change and not much chance to test

Scope

- Out: Government personnel (policies dominate)
- Out: Extremely high risk (no chance)
- Out: Very low risk (better security choices)
- In: “Goldilocks” region of just-right risk

What factors influence Risk?

- Targeting specificity
- Attack technique intrusiveness
- Persistence of compromise
- Attacker: hostility and resources
- Consequence of failure
- Defender resources
- Degree of exposure to attack

Targeting Specificity

- General/ambient in environment
- Person or organization in a category
- Specific person or organization of interest

Technique Intrusiveness

- Passive network attacks (sniffing)
- Active network attacks (injection, remote “hacking”)
- Physical non-destructive access
- Physical modifications/tampering
- Multi-touch physical modifications

Persistence of compromise

- Only “current” data
- Historical data
- Future/ongoing system access

Attacker hostility/resources

- Both absolute and relative focus:
- A very capable organization with little interest
- Less capable organization with extreme interest

Consequence of failure

- Lives at risk
- Criminal liability or imprisonment
- Commercial net return for attack
- Property destruction or loss
- Disruption or inconvenience

Defender resources

- Government
- “Platform developer” or security organization
- Well resourced enterprise
- Resourced organization (commercial or non)
- Individuals or shoestring activists

Degree of exposure

- Large user population
- Frequency of travel
- Lots of infrequent travelers
- User training and general security awareness
- Legal exposure/status

How high risk?

- Out-high: North Korea (risky/restrictive/rare)
- Probably out: Active conflict zones (e.g. Syria)
- Borderline-high: US/EU to Russia
- **Now relevant: (some) EU people visiting US**
- Out-low: Domestic US or EU (too safe)

Sweet Spot: China

- Western people and organizations visiting
- Generally commercial targets, not intelligence
- Substantially law-abiding, international relations
- High volume of travel, travel important
- Technically sophisticated adversary

General goals:

- Avoid special treatment/targeting
- Resist attacks in proportion to difficulty
- Limit information at risk of exposure
- Don’t piss them off if targeted
- Use technology for leverage to increase defense

Techniques

- Substantial overlap with best “conventional” security practices
- Unique: the idea of a “safe” vs. “unsafe” time and place
- Finite duration of time at heightened risk

Minimize threat surface

- Limit the amount and variety of equipment exposed
- Organizations often have “travel pools” of dedicated hardware for international travel

Prepare systems in advance

- Auto-updates and in-field modifications are not your friend
- Implement system hardening best practices per platform (some good guides available online)

Minimize data

- Don’t carry **all** your data if you don’t need it!
- Cross borders with no data, only tools, and download-it-there

Protect home/future

- Don’t bring long-lived credentials
- Don’t bring credentials with unneeded access
- Don’t allow system compromise to pivot to home

Protect personal accounts

- Don’t focus solely on corporate/organizational accounts
- User personal accounts (Twitter, Facebook, email, etc.) can be used for a variety of attacks
- Consider exceptions to policies about work/personal separation while traveling

User training

- Top priority for users is “get the job done”
- Often will compromise/work around security if needed to accomplish top priority
- Make the most secure way also the easiest way
- Great network access good inducement

So, what works?

- China-specific VPN services often work (but inconsistent/always changing, no recommendations)
- International roaming cellphones/data service
- Dedicated pools of travel equipment often work if managed well, but challenging
- Tools which enforce non-permanence

What doesn’t work?

- “Special” hardware gets you special treatment…
- Google Chromebooks are problematic due to dependence on Google services
- Desktop-as-a-Service: latency/connectivity issues
- Many US-hosted services are dependencies
- Free/commercial public VPNs often blocked
- Some corp VPN/etc. protocols blocked

Stuff which fails often

- Full disk encryption doesn’t work vs. “decrypt this or else” in many countries (still do it!)
- Secure messengers w/ history (“unlock/show!”)
- Complicated systems which depend on user actions often don’t work
- Things which work in one location often fail elsewhere
- Often must continue using even a suspect system

Future R&D

- Better VPN
- Better Desktop as a Service (DaaS)
- Better Laptops
- Better Phones
- Better Management/Visibility

Better VPNs

- Split between “public/free” and commercial/dedicated is fundamental
- Optimized protocols
- Lots of great work from Tor transports
- Hardware appliances vs. software clients

Better Desktop as a Service

- Network tolerant: Latency, bandwidth, jitter, loss
- Proximity of DaaS servers, connectivity
- Hardened DaaS servers
- Communications-optimized applications

Better laptops

- Disposable?
- Easily wiped/restored in field to good state
- Tamper-evident or tamper-responding
- Easily inspected/centralized state on device
- Reduced functionality, higher baseline security

Better phones

- Disposable?
- Phones are great: easy to keep with you
- Baseband risk
- Hostile carrier risk
- Lack of virtualization, single instance of app
- MDM is good but challenging w/ network
- Backups/reinstallation in the field, full image/restore hard
- iTunes/iCloud or Google store is problematic

Management/Visibility

- It is possible to assemble and operate a decent system today for China travel and similar threats
- Very challenging to do it at small scale, or with limited resources
- Very expensive/time intensive to maintain even in larger organization
- Most conventional management tools not ideal

Sales pitch to activists

- Full rights as close to the border as possible
- Push governments to treat visitors well
- Publicize abuses at the border or against visitors

FOX

Conclusion

- Happy to talk about specific travel needs, especially for organizations with multiple users, history of being targeted
- Putting together centralized links to best practices for various applications and platforms
- Anyone interested in the “R&D areas” please get in touch

How the US has changed

- Donald Trump’s election in November 2016
- Travel bans against certain origin countries
- Laptop bans in cabins of certain flights
- General heightened suspicion and distrust

Good news about US travel

- Media remains very active
- Legal challenges ongoing
- Lots of activist and industry attention
- On paper, legal protections remain very high

Bad news about US

- Policies vary widely by airport/port of entry
- Individual agents have wide discretion
- Attacks are targeted at those least able to resist
- Hackers appear to be targets