Security in the age of Softphones

1) Towards a new security model

2) Towards definitions of malware

3) Traditional privacy notions in the age of smartphones

Greg Troxel <gdt@ir.bbn.com>

Copyright 2015 Raytheon BBN Technologies
Towards a new security model in the age of smartphones

Greg Troxel <gdt@ir.bbn.com>

Copyright 2015 Raytheon BBN Technologies
Traditional model

- Confidentiality, Integrity, Availability
  - Still makes sense, but is not sufficient
- Access, Boundaries (closer)
- Key assumption often unstated
  - Single entity with control and security goals
    - two computers and data transfer between them
  - Adversary is external to the two computers
  - Computers are under the control of and act in the interest of the computer/data owners!
  - Implies software acts in the interest of the owner of the installed computer...
Running other's code

• Before, the default assumption was that a program did what it said, and acted on behalf of the uid running the program.
  – An obvious exception was virus/trojan code; there was a vast divide between “program you wanted to run” and “malware you didn't want to run”

• Now, that assumption is unsound, particularly in Mobile
Agency defined

- We define a new security service, *Agency*, which is (for now) about programs.
  - (I need a better word.)

- A program has Agency if it, absent bugs, acts in the interest of the person on whose device (under whose uid) the program runs, in the view of a knowledgable, disinterested third party.
  - This is a social/legal definition, not a technical one!
  - This is very similar (perhaps the same as) the notion of fiduciary responsibility;
Traditions: Free Software

• While not intrinsic to the definition, most in the community would object to a program lacking agency, modulo relatively minor edge cases about version reporting and statistics.
  – History of vulnerability reports for lack of agency (tracking)
  – f-droid.org labels programs for various issues
  • https://f-droid.org/wiki/page/Antifeatures “Antifeatures are flags applied to applications to warn of behaviour that may be undesirable from the user's perspective. Frequently it is behaviour that benefits the developer or third party, but that the end user of the software would prefer not to be there.”
Traditions: Proprietary Software

• Traditional Proprietary Software is expected to mostly have Agency, with the exception of license enforcement.

• Most license-related Agency failures are straightforward, rather than hidden.
The strange world of mobile

• In Mobile, it is for some reason common to run code from untrusted third parties, and then try to contain what it can do (or to trust them incorrectly!)
  – Implicit in this mindset is a lack of confidence of Agency
  – Also implicit is that app permissions can mitigate a lack of Agency, but
  – The real issue is semantics and intent, and ultimately access to data
  – How do Agency failures relate to incentives and the advertising business model?
Towards definitions of malware in the age of smartphones

Greg Troxel <gdt@ir.bbn.com>

Copyright 2015 Raytheon BBN Technologies
What does malware mean?

• Before, it meant membership in one of a set of classes, e.g.
  – “Virus”
  – Trojan
  – Botnet client
  – Keylogger/APT/exfiltration

• Lack of Agency is so obvious it is not discussed
Examples

• Uploading address book to server (without explicit user request)

• Reporting location to third party when not clearly related to user behavior
  – todo: insert examples

• Use of data for app author's purpose, not app user's purpose
Malware redefined

• Malware is code that fails the Agency property.
  – Arguably shades of gray are needed; some failures are more serious.

• Much javascript from websites is likely malware under this definition.
Traditional privacy notions in the age of smartphones

Greg Troxel <gdt@ir.bbn.com>

Copyright 2015 Raytheon BBN Technologies
Traditional privacy notions

- Before, many norms were
  - Obvious, so no one thought to ask that they be followed
  - Technically difficult or required great effort to violate
- Now, old norms are often not followed
  - Asking people to follow them can be odd
  - People's phones violate norms without the owner's knowledge
    - What's the difference between this and (prohibited) electronic surveillance?
Causes for problems

- Agency failures
  - Softphones act without owner's knowledge and consent

- Technically easy oversharing
  - It's too easy to be overshare other people's information by accident

- Differing opinions about norms
  - Oversharing your own information, vs. that of others
Geotagged Photos

• Before: someone visits, takes photos, writes your address on them, and posts them on the local library bulletin board
  – In 1995, no one would think to do that, or think it was necessary to ask guests not to
• Now: configuration for auto-publishing on social networks, photo sharing sites, etc.
  – Would you do this without asking?
  – Do you ask people not to do this?
  – Would you think being asked not to is odd?
Reporting location to ad companies

• Before: someone visiting uses your landline to call an ad company's 800#, and reports your address (so it can be looked up for other calls)
  – In 1995, this is unthinkably rude.

• After: Google Location Services reports GPS-derived coordinates for wifi BSSIDs. Code (malware!) in various apps reports coordinates to geolocate the public IP address.
  – Would you do this without asking?
  – Do you ask people not to do this?
  – Would you think being asked not to is odd?