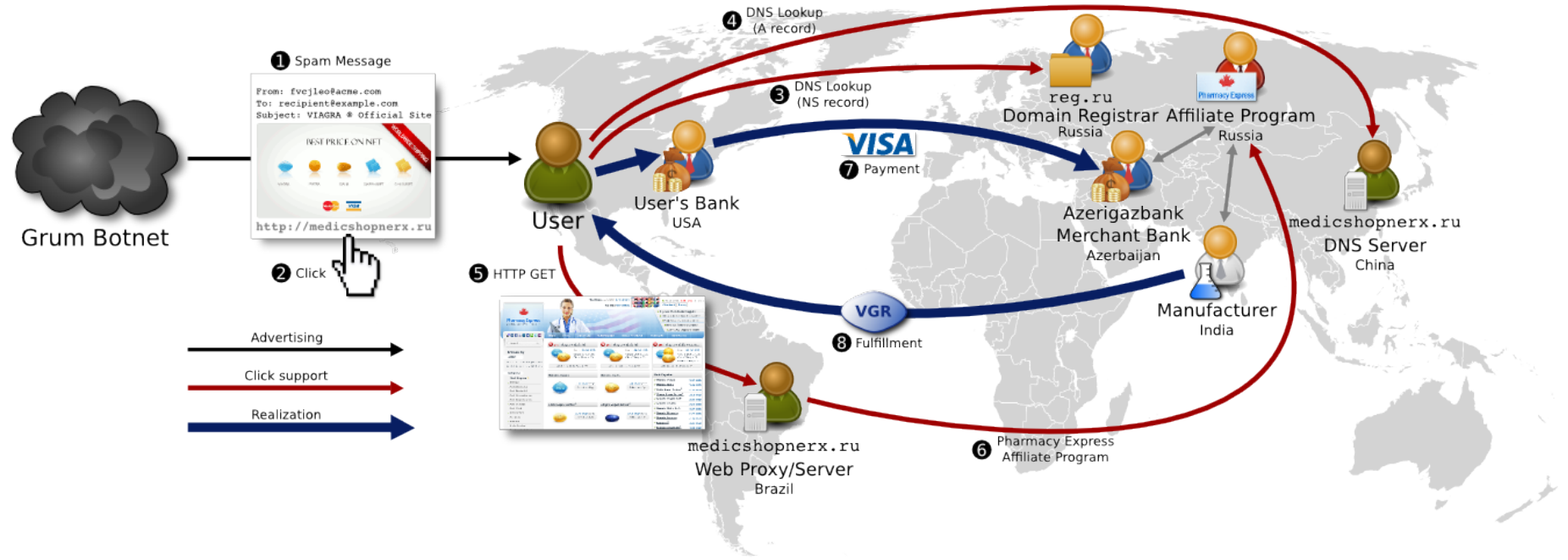
Workshop on Extensible Distributed Systems

Security Panel

Geoffrey M. Voelker

January 21, 2015

(Coming from Cybercrime)



Security Ramblings

- Large-scale pervasive distributed systems
  - Vision is incredible
  - Security is incredibly scary
- Who wants to attack pervasive systems?
  - Not just how a system can be hacked, but why
- End with a laundry list of thoughts/challenges
  - And by “challenges”, I mean questions

Researchers

- Automobiles, voting machines, pacemakers, airplanes, cameras, …
- Unless a system receives security pressure, it is going to be more vulnerable
  - Research applies that pressure before attackers
  - (“Experimental Security Analysis of a Modern Thermostat”)

- How to experiment with devices? (pacemakers…)
- How to navigate issues on reverse engineering?
- How to fund?

Profiteers

- How will people profit from hacking pervasive devices?
  - Target (oh so ironically named) a good example
  - (Thermostat? Hmm, how can an attacker monetize?)

- Can we proactively/predictively use lessons learned from existing cybercrime activity?

Tracking/Surveillance

- Industry and government
- Pervasive devices → Unprecedented ability to track what people do, when, where, etc.
  - Google knows what you browse
  - LG knows what you watch
  - Sears knows what's in your fridge
- How to reason about privacy when everywhere you go, everything you do is logged?
  - Medical devices alone are a compelling domain

Nation State

- Tracking and surveillance
- Disruption
- Cyberwarfare
- Censorship

- Adding pervasive systems into the picture only makes the situation worse
- How do you secure pervasive systems when the adversary has the deep pockets of a national government?

Challenges

- Fault tolerance & security: Chocolate & peanut butter?
  - FT a hallmark of distributed systems
  - How can security take advantage of redundancy, failure detection, etc., that distributed systems provide so well?
  - (And vice-versa: anomalies as failures)

- Detecting attacks
  - Run anti-virus on every device? (Norton ToasterAV)
  - Run IDS on every embedded network? (CarBro)
  - Is there a more holistic approach incorporating information across devices, networks? (ADT Cyber)
    - » Take advantage of pervasive to improve security/privacy?

More Challenges

- Devices/systems will be hacked
  - How to respond?
    - » May not be able to update devices (e.g., cars)
  - Safety becomes a real issue (medical devices)
    - » Tend not to consider in typical Internet security

- How to get pervasive device ecosystem to adopt security practices?
  - (Which we can't even get traditional platforms to adopt)
    - » (Amazes me that we don't use CFI, XFI, etc.)
  - Ray of hope: PL, formal verification finally ready?

Even More Challenges

- Human factors: Usability, understandability, flexibility
  - How do users define/select security, data policies?
  - Medical devices particularly challenging
    - » Private but for authorized access (doctor, nurse)…but also emergency access override (EMT)…insurance gets access?

- Security metrics (sorry, makes me cringe, too)
  - How do we quantify whether security is better?
  - (Price of commodities on underground markets…)

Grand Challenge?

- "… an exa-op data center that consumes no more than 10 megawatts (MW), a peta-op departmental server that consumes no more than 10 kilowatts (KW), a tera-op portable device that consumes no more than 10 watts (W), and a giga-op sensor system that consumes no more than 10 milliwatts (mW)." [Hill]

- Can we articulate a similar grand challenge in terms of security?