Internet Governance and Culture

David D. Clark

MIT CSAIL

November, 2017

My starting point today: security

- Security is a critical issue for the future of the Internet.
- Why is security a persistent problem?
  - Why don't we just fix it?
- The points of my talk:
  - The word security is not actionable.
    - Aspirational, not operational.
  - Most of our security problems are not technical.
    - If they were, we *would* have fixed them.
  - The barriers to better security often involve issues of incentive, coordination, global scope, mis-aligned interest, and un-trustworthy actors.
    - These are the issues we must address to improve security.
  - Nobody is in charge.
    - And that is the secret of the Internet's success, but as well perhaps its deepest challenge.

First challenge—define security

- “Security” is not a well-defined objective.
  - Just a high-level aspiration.
- There is sub-structure to the goal of security.
  - And once we unpack the concept, we find conflict and tension among the sub-goals.
  - Security is about balance, not perfection.
  - Balance among goals, balance among actors

Factoring the security challenge

- Trusting users try to communicate
  - Untrustworthy elements attack the communication.
  - Could be a network operator, for example. (Or NSA…)
- One user attacks another.
  - As part of intentional communication.
  - Without any desire to communicate with the attacker.
- The network itself is attacked.
  - One part attacks another.
  - Users attack the network.
- Denial of service attacks.
- I will extract some case studies from this list.

Attacks on communication

- Use the classic security sub-goals:
  - Confidentiality
  - Integrity
  - Availability
- Cryptography is a powerful tool
  - Encrypt content -> confidentiality protected.
  - Signed content -> loss of integrity detected.
- Encrypted communication is used in several ways in the Internet.

Cryptography

- Standards:
  - NIST, NSA. Works well.
- Software:
  - Underfunded open source project.
  - Incidents of major flaws.
- Key management: cryptography depends on keys.
  - Where do keys come from and how are they managed? Use Web as example.

Internet key distribution

- To over-simplify massively…
  - Keys are managed through the Certificate Authority system.
- When a browser connects to a secure web site, the site sends a *certificate* to prove who it is.
- A certificate contains (to simplify):
  - The DNS name of the server.
  - The name of the organization.
  - The public key of the organization.
  - ID of trusted third party that vouches for this information.
    - Cryptographically signs it.
    - These trusted third parties are called *certificate authorities (CAs).*
- But who vouches for the third party.
  - Need the key for *that* actor.

Trust hierarchy

- A CA vouchs for a server.
- A “higher-layer” CA vouchs for that first third party.
    - And so on.
- But there has to be a shared agreement about the “highest-level” CAs for this scheme to work.
    - Roots of trust.
- How does a client today know about the top-level CAs?
    - The list comes pre-loaded in the browser.
    - The real root of trust is the distributor of the browser
        - Mozilla, Apple, Microsoft, Google

The flaw in the scheme…

- What if a CA is actually not trustworthy?
  - Issues false certificates?
    - CA could be corrupt, penetrated, or adversary.
  - Does this happen in practice? YES!
    - Dutch CA DigiNotar was penetrated, apparently by Iran.
    - Google recently declared China CA untrustworthy after false certificates were used in an attack on TLS-protected communication.
    - Google-China interaction rises to level of high politics.
- What if someone slips you an extra “trusted” root certificate?
- Generalization: most uses of crypto are embedded in a larger context of key management, trust, etc. The flaws are there.

Who is in charge?

- System (mis)-designed as a globally distributed system with no central point of control.
  - Poor tools to discipline an untrustworthy actor.
  - Reality: must assume some actors are untrustworthy.
- The CA/Browser Forum (an industry group) makes decisions about what root CAs to put into browsers.
  - But providers of devices (cell phones) can add extra root CAs.
  - How can that behavior be disciplined?

Untrustworthy users

- The previous problem:
  - Users trying to communicate are attacked by network element.
  - Implication: they had interests in common and were mutually trusting.
- The reality of today:
  - Most communication on the Internet is among parties that do not trust each other and with good reason.
    - Email: spam, phishing, malicious attachments.
    - Web: forged web sites, downloaded malware, profiling.
  - But on balance, users proceed.

The network and the application

- The network, by design, is general.
  - It does not know what the users are trying to do.
  - It just moves sequences of packets.
- Applications, by design, define the actual flows of data.
  - Applications define the experience of using the network.
- The network *should not* know what the users are trying to do.
  - Would make it easier for net to attack users.
  - Might raise barriers to deployment of apps.
- Applications are complex.
  - Likely to have risky modes of operation.

Applications: insecure by design?

- Users favor features over constraints.
  - Sending arbitrary attachments in email, downloading Javascript, etc. is very useful.
  - Makes good sense when parties are prepared to trust each other.
  - Users favor both features and availability over potential security concerns.
- Possible design approach for apps:
  - Vary feature set depending on degree of trust.
  - “Don’t accept Javascript or attachments from strangers”.

Again, who is in charge?

- No regulation of applications.
  - Anyone can build one.
  - That was the power of the Internet.
  - A global market.
- Moving key security challenges into the core of the Internet would be a Very Bad Idea.
  - Should the net police applications?
  - Should the net try to enforce mandatory identity?

Internet governance

- To understand governance of Internet security, must understand overall governance.
- Highly decentralized.
- Bottom up structure.
  - Groups form to solve problems.
- A brief history lesson.

In the beginning…

1974-1981: There was a small band of federally-funded researchers, including Jon Postel.

Jon and Joyce Reynolds gave out blocks of addresses and domain names on request.

1988: This activity was formalized under a contract with the U.S. DoD as the Internet Assigned Number Authority, or IANA.

1986: Original research team reorganizes itself into a number of working groups as the Internet Engineering Task Force (IETF) and an oversight steering group, the Internet Activities Board (IAB).

IANA in the 1990's

First delegation of address assignment to Regional Internet Registries (RIRs):

1992:Réseaux IP Européens (RIPE)

(Founded by network operators in 1989)

1997: American Registry for Internet Numbers (IANA)

- Now five RIRs: AFRINIC, APNIC, LACNIC

1999: Transition of the IANA function to Internet Corporation for Assigned Names and Numbers (ICANN), funded by U.S. Dept. of Commerce.

- Complex dance with RIRs to accept the authority of ICANN.
  - To our great distress, Jon died in the middle of negotiations.
- Dance completed in 2003.

IETF in the 1990’s

- 1993: Internet Society is created as a corporate shell for the IETF. Private, non-profit U.S. corporation.

Operations governance in 1990’s

Network operators have a need for coordination and sharing of knowledge.

1994: North American Network Operators Group (NANOG) first meets.

- Outgrowth of NSF-funded Regional-Tech meetings (organized by MERIT).

2010: NANOG becomes independent of MERIT.

Governance regimes

- Names and addresses: ICANN and RIRs
- Standards-setting: IETF and Internet Society
- Operations: NANOG
- Other examples:
  - Dealing with abusive behavior :Messaging, Malware and Mobile Anti-Abuse Working Group (*M^3AAWG*)
  - Oversight of Certificate Authority system: CA/Browser Forum (2005)
  - Interconnection: IXes and associations.

What do they have in common?

- Bottom-up, self-organized.
  - ICANN is partial exception.
- Authority is earned, not given.
  - Earned through demonstrated competence.
  - Careful management of governance.
  - Control of “mission creep”.
  - Trust is central.
- Internet governance runs on beer.
  - The Pakistan episode.

Meanwhile, around the world

China notices the Internet.

- Tradition of top-down, state centered governance.
- No experience or comfort with bottom-up, multi-stakeholder processes.
- Strong believe in priority of sovereignty.

- China is pushing very hard to shift international governance of the Internet to a top-down, state-centered approach.

China timeline (partial)

2003: calls for replacement of multi-stakeholder model of governance with Int'l Internet Treaty and formation of Intergovernmental Internet Org: first WSIS

2010: Internet White Paper - "Within Chinese territory the Internet is under the jurisdiction of Chinese sovereignty. The Internet sovereignty of China should be respected and protected.”

2012: WCIT 12.Push for revision of governing treaty of International Telecommunications Union (ITU) to give it authority over international character of Internet.

2015: 40 delegates to IETF.

2016: 2-yr plan to build/upgrade telecom networks in Africa $173B

- State-centered regulation gives each country one vote.
- The African voting block very important to Chinese ambitions.

Now: cyber-security

- Must unpack “security” to make progress.
  - Would expect different institutions to focus on different problems.
- How many governance institutions can we find?
  - A project of my graduate student, Cecilia Testart.
- Answer: The space is over-populated with governance organizations with low levels of earned authority.

Finding the institutions

- Start with a venue with diverse participation.
  - IGF
- Study the transcripts of all the sessions.
  - Use automated tools.
- See what people mean when they use the word “security”, and see what institutions they mention.
  - Then see how they define themselves.
- Follow the leads.
  - A sort of snowball sample method.

Where did she end up?

- Defined “governance” broadly:
  - Is the institution shaping Internet security?
- 120+ institutions and counting.
  - Never find them all, but an interesting (and hopefully representative) sample.
- Seems, if anything, “over-institutionalized”
  - And yet, security is a persistent problem.
- Why so many, and what do they do?
- Reflects differences in:
  - The sub-problem to be solved.
  - The organization approach.
  - The scope (domestic or international).

Competing governance models

- Top-down and bottom-up do not mix well.
  - Authority granted vs. authority earned.
- Top-down governance is not trusted and often demonstrabily lacking in competence.
- Bottom-up governance hesitates to take leadership position.
  - Can be seen as mission creep and can erode their existing authority.
  - Nobody is in charge.
- Contention between domestic and global responses.
- The challenge: find a way for leadership to emerge that can define a way forward.

Leadership

- Realist theory predicts that those who have power will use it.
  - Who has demonstrated power here? Google.
    - Google vs. China over abuse of the Certificate Authority system.
    - Google intervention to stabilize Certificate Authority system
  - Governments have to learn how to lead through soft power, not by claiming they are in charge of the international system.