U.S. National Cybersecurity

Policy 101

William J. Perry
Martin Casado · Keith Coleman

MS&E 91SI
Fall 2006
Stanford University

Brief History of the Internet: What and Why

The Beginning

1967

- Defense Dept (through ARPA) funds ARPANET project
- ***Why?***
  - **An Inspiration:** Foster community among disparate research centers
  - **A Need:** Avoid wasteful duplication of computer resources → share instead
  - **Not:** For communication in nuclear incident
- Only government actually wants this; everyone else is ambivalent
- Government just says “build it”
- Design left to informal Network Working Group (NWG) made up of researchers, grad students, contractors, etc

Owned by	Government (ARPA)
Designed by	Government Contractors (NWG)
Developed by	Government Contractors (BBN, Researchers)
Operated by	Government Contractors (BBN)

Opening and Commercialization

1970s & 1980s

- Communication turns out to be the killer use (e.g. Email)
- Surprise innovations driven by users (e.g. WWW, email)
- ***Competition in design***
  - Govt seeds design consortiums with competitors
  - Consortiums decide by consensus → generic platform
- ***MILNET/ARPANET split***
  - Military needs secure system, so it splits to preserve open ARPANET
- ***Govt as a VC***
  - $20 million fund for companies that implement TCP/IP into software

Owned by	Government (ARPA)
Designed by	Everyone (Open design consortiums)
Developed by	Everyone (Govt contractors, private sector)
Operated by	Government Contractors (BBN)

Ready for Release

1980s and 1990s

- ARPANET decommissioned, traffic moved to new NSFNET backbone
- ***Formalized Open Design***
  - Merger creates IETF, IAB – open design and discussion groups
- “Internet“ becomes a reality (and internationalization)
- Commercial dial-up and use begins (can order from PizzaHut.com)
- NSF prepares plans to hand operation over to private sector

Owned by	Government (NSF)
Designed by	Everyone (Formal open design consortiums)
Developed by	Everyone (Govt contractors, private sector)
Operated by	Government Grant Awardees (MCI, Universities)

Today's Internet

1995

- NSF backbone shuts down
- 4 commercial ISPs take over
- ***End of government ownership of Internet infrastructure***

Owned by	Everyone (Backbone ISPs, private/public networks)
Designed by	Everyone (Formal open design consortiums)
Developed by	Everyone (Govt contractors, private sector)
Operated by	Everyone (Private sector, universities)

Tomorrow’s Internet

2006

- Mania to redesign a better Internet

- GENI: Global Environment for Network Innovations
  - “GENI is an experimental facility being planned by the **NSF**, in collaboration with the research community. It's goal is to enable the research community to invent and demonstrate a global communications network and related services that will be qualitatively better than today's Internet. The research community is encouraged to participate in its design.”
  - http://www.geni.net/

- Clean Slate Design for the Internet
  - "With what we know today, if we were to start again with a clean slate, how would we design a global communications infrastructure?“
  - "How should the Internet look in 15 years?”
  - http://cleanslate.stanford.edu/

Where Are We Now?

Open, commercial Internet.
Government can influence through:

Law

- Basic rules governing what is legal/illegal
- Legislation or case law
- We'll use it primarily in reference to rules governing individuals

Industry regulation

- Legislation or government action resulting from legislation that intends to modify or control the behavior of an industry or other large entity
- Not inherently good/bad, pro-/anti-business

Initiatives

- Government action to work with industry or other major actors to improve cybersecurity
- May be in the form of legislation

Law

Computer Fraud and Abuse Act

- Passed in 1984
- Most comprehensive law regarding computer crimes
- Defines specific felonies, including…
  - Using computers to obtain classified information
  - Using computers to defraud others
  - Damaging or denying service to computers used in Interstate Commerce or Communications
- Morris, Mitnick, etc.

DMCA

- Makes it a crime to produce or disseminate technology that can circumvent copyright protection mechanisms
- Don’t need to infringe copyright to commit a crime
- Security implications?
  - Cannot research software to ensure provides appropriate protection mechanisms (Felton v. RIAA, Sklyarov v. Adobe)
- Strongly supported by media industries

UCITA
(Uniform Computer Information Transactions Act)

- Initial purpose: ‘bring uniformity and certainty to the rules that apply to software transactions’
- ‘shrink wrap’ licensing
  - Release rights before use
  - Courts sometimes disregard
- Remote disablement
- Protection from knowingly distributing buggy software
- Must be enacted independently in each state

CoE Convention on Cybercrime

- International agreement requiring
  - Nations must cooperate on cybercrime investigatoins
    - Mandatory even if the act is not illegal in both countries
    - US can deny if speech or other rights would be violated
  - Nations must develop similar domestic cybercrime legislation addressing intrusion, fraud, child porn, …
- Opponents say it authorizes sweeping investigative powers without judicial approval
- Signed by Europe in 2001, Bush in 2003, ratified by U.S. Senate in August 2006

Industry Regulation

Ex #1: FISMA

Federal Information Security Management Act (FISMA):

Goal:

Strengthen federal agencies resistance to cybersecurity attacks and lead by example.

What is it:

Mandates that CIO of each federal agency develop and maintain an agency-wide information security program that includes:

- periodic risk assessments
- security policies/plans/procedures
- security training for personnel
- periodic testing and evaluation
- incident detection, reporting & response
- plan to ensure continuity of operation (during an attack)

Yearly report to Office of Management & Budget (OMB)

Ex #2: HIPAA

Health Insurance Portability and Accountability Act (HIPAA)

Goal:

Secure protected health information (PHI),

What it is:

- Not specific to computer security at all, but set forth standards governing much of which is on computers.
- Insure confidentiality, integrity and availability of all electronic protected health care information
- Comprehensive: ALL employees must be trained.
- Does not mandate specific technologies, but makes all “covered entities” potentially subject to litigation.

Government Initiatives

Ex #2: National Strategy to Secure Cyberspace (2003)

Goal:

Outline U.S. strategy on cybersecurity and "empower all Americans to secure their portions of cyberspace."

What is does (highlights) :

- Stresses importance of public/private partnerships
- Focus on awareness/information deficit surrounding cybersecurity
- Recognizes government role as facilitator of research and industry collaboration.

Ex #2: Cyber Security R&D Act (2002)

Goal:

Promote research and innovation for technologies relating to cybersecurity and increase the number of experts in the field.

What is does:

Dedicated more than $900 million over five years to security research programs and creates fellowships for the study of cybersecurity related topics.

Ex #3: Critical Infrastructure Information Act of 2002

Goal:

Reduce vulnerability of current critical infrastructure systems

What is does:

Allows the DHS to receive and protect voluntarily submitted information about vulnerabilities or security attacks involving privately owned critical infrastructure. The Act protects qualifying information from disclosure under the Freedom of Information Act.

Ex #4: US-CERT (2003)

Goal:

Coordinate defense against and response to cyber attacks.

What is does:

- CERT = Computer Emergency Readiness Team
- 24/7 contact point for industry into the DHS and other gov’t cybersecurity offices.
- National Cyber Alert System
- National Cyber Response Coordination Group

Who are the government players?

Gov’t Cybersecurity: Then

1996:

President Clinton established the President’s Commission on Critical Infrastructure Protection (PCCIP).

1998:

Clinton administration issued Presidential Decision Directive 63 (PDD63) creates :

- National Infrastructure Protection Center (NIPC) in FBI
- Critical Infrastructure Assurance Office (CIAO) in Dept. of Commerce

2001:

After 9/11 Bush creates:

- White House Office of Cyberspace Security (Richard Clarke)
- President’s Critical Infrastructure Protection Board (PCIPB)

Gov’t Cybersecurity: Then

2002:

Cybersecurity duties consolidated under DHS -> Information Analysis and Infrastructure Protection Division (IAIP). Cybersecurity chief is a mid- to low-level position.

2003:

National Cyber Security Division (NCSD) created under IAIP. Role of the NCSD is to conducting cyberspace analysis, issue alerts and warning, improve information sharing, respond to major incidents, and aid in national-level recovery efforts .

The United States-Computer Emergency Readiness Team (US-CERT) is the United States government coordination point for bridging public and private sector institutions.

Gov’t Cybersecurity: Now

2005-6:

DHS has churned through 5 cybersecurity czars in 3 years (Clarke, Schmidt, Yoran, Liscouski, Purdy). No one can get anything done, no one wants the job.

After Congressional vote, DHS agrees to re-orgs and raise level of cybesecurity division. Cyber chief is now an Assistant Security position reporting to Undersecretary of Preparedness.

Sept 18, 2006 – DHS ends 14 month vacancy, hires Gregory Garcia as new Assistant Secretary for Cyber Security and Telecommunications.

Other Gov't Actors

Congress:

Funding & Legislation

House:

- Committee on Homeland Security -> Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity
- Committee on Science

Senate:

- Committee on Homeland Security & Government Affairs
- Committee on Commerce, Science & Transportation

Other Gov't Actors

The usual suspects:

- FBI
- Secret Service (DHS)
- Dept. of Defense
- NSA (DoD)

and don't forget:

- DOE
- Dept. Commerce / NIST
- SEC
- FCC
- Dept. of Treasury
- Office of Management And Budget (OMB)

and more...

The Big Picture

What's the Point?

Complex web of interactions. There are many different government actors with their own interests and specialties

No single leader

Discussion

Questions

Think about what is possible?

- International?
- Lack of metrics?
- Not feasible/useful? (Utah banning porn on port)

What are benefits of certain types of regulation?

What are drawbacks?

We’ll look at this in more depth in the discussion.

Student Discussion Questions

Nick Miyake

Would it be unreasonable to require computer owners to possess a license? Or require some kind of preliminary training course before you can sign up for an Internet connection? We require licenses in order to drive, and it works out fine -- pretty much everybody has a license and it isn't a big deal. There are obviously huge problems as far as implementation goes and privacy may also be an issue, but what do people think about the underlying idea? When cars first came out, I doubt that people needed licenses to operate them. However, as they got bigger, faster, and became a greater part of the country, the government started to regulate. Seeing that many consumer computers are at the point where supercomputers that were classified as weapons (placed under export restrictions, at least) a few years ago are, it doesn't seem unreasonable to regulate their purchase or use.

John Cieslewicz

The article by Oram suggests the role that insurance may play in securing cyberspace. Insurance companies often require certain standards to qualify for policies and actively check up on their clients' performance (I'm thinking of fire, earthquake insurance here where building improvements, etc. are often required by the insurer). Could insurance be a solution? Could it result in security practices where insured entities aim to meet the bare minimum security requirements set forth by the insurance companies, knowing that any liability or damage resulting from other security problems will be covered by the insurance company? By the same reasoning, could insurance company or any other regulations (i.e. government regulations) cause common vulnerabilities or failures among entities with computer and/or network systems?

Student Discussion Questions

Joseph Lin

how much does democracy, and the realities of election politics limit the administration's ability to enact tough (and perhaps necessary) legislations?

Olivia Billett

The government and DHS both agree on the importance of communication with and support of industry. From the GAO report - "Because a large percentage of the nation's critical infrastructures is owned and operated by the private sector, public/private partnerships are crucial for successful critical infrastructure protection." Given that they recognize the need to secure industry as well, why did the US cybersecurity plan shy off from requiring industry regulation? Expense was the only issue mentioned, but is it not worth some government subsidy to ensure that industry meets required security minimums?

Notes on “Inventing the Internet”

- Built because: (p43)
  - Inspiration: Foster community among disparate research centers
  - Need: Avoid wasteful duplication by providing access to specialized gov’t bought research computers (previously had to buy them for each research center, now they can share. ARPA payed for the all anyway)
- 1967 Project funded by ARPA to link research centers of contractors
- Network Working Group [NWG] develops software specs – made up of grad students P. 59 – disbanded in 70s but model continues (206)
- Design consortiums seeded with competition (71, 145)
- BBN runs the network (p 64)
- Early 70s: Email – ARPANET is now about communication, not sharing (111)
- 1982: Split into MILNET (with encryption and security) and ARPANET (open) (143)
- Effort to commercialize: ARPA as VC ($20 million fund to ifnance mfctrs to implement TCP/IP) → by 1990 available on nearly every computer (143)
- 1990: ARPANET decommissioned, NSFNET becomes backbone (195)
- 1991: NSF develops plan to hand over to competing ISPs (196)
- 1994: Pizzahut.com
- 1995: NSFNET backbone shut down, four ISPs take over – end of government ownership of infrastructure

- IAB (Internet Activities Board) created – open discussion on internet policy (207)
- NSF and ARPA merger creates IETF
- 1992: Internet Society leads IAB and IETF

Notes on “Inventing the Internet”

- Key ideas:
  - Open design methodology
  - Competitive design methodology (govt put competing organizations on design committees)
  - Competition in operation (not one ISP, but four competing ISPs)

  - computer sharing turned out to be somewhat useful, but many of the most successful applications were spawned as random user creations (email, www, etc) made possible by a policy of extreme openness
  - design team was a consortium of people with competing interests. Design team internalized competitive market forces by encompassing so many diverse members (university researchers, isp corporations, military officials, etc) and made decisions based on consensus, which led to a system that accommodated many needs, uses and requirements. (This is one explanation given for the Internet’s success over competing private commercial networks—that the nature of its design made it a nearly ideal, generalized platform for so many different types of users.)
  - Government acted almost like VC – offered venture-like product-level funding for companies that produced products compatible with TCP/IP. Every major company took the funding and soon nearly ever major OS supported the protocol.
  - Project had budget model of military (e.g. cost is no object) yet development style of research institutions (elegance over short-term profit) – basically, stuff was done right.
  - Allowed easy growth at periphery—government even helped people create LANs and regional local networks. This leads to network effect—more users demand more services which begets more users, etc.

- One of the most interesting things about the Internet project is that the government mandated ARPANET creation but from there on out never mandated design specs. ARPA wanted something that accomplished the goals (and presumably funding was dependent on this) but it does not appear as though government ever made design requirements or design vetoes. All design decisions were made by the ARPANET’s users.

SOX & GLBA