Introduction
Introduction to the introduction

CSCI E 45a: The Cyber World – part A

Welcome to
CSCI E 45a: The Cyber World – part A

The cyber-world @ Harvard Extension

- This is one of a pair of courses we teach
- Each course stands alone
- They can be taken in either order

Not just security!

E45a focuses on the foundational building blocks: hardware, software, networks, security fundamentals, and history

E45b focuses on the real world: privacy, trust, surveillance, threats, conflict, commerce, etc.

The cyber-world @ Harvard Extension

- These two courses are on the optional list for the Harvard Extension Cybersecurity Certificate
  - With these two courses, you are half-way to the certificate.
  - To complete the certificate you need two courses from the list of required courses taken within three years, scoring B or better

Learning goals

- This module is for you to:
  - Get to know us, the instructors
  - Understand what this course is about
  - Understand what our goals are for teaching this course
  - Understand the logistics, and practical aspects of taking this course
  - Get an overview of the content of the course

Topics

- Scott - O
  - A brief introduction to Scott
- Ben - O
  - A brief introduction to Ben
- Course logistics - R
  - All the practical details you should know about this course
- Exams - R
  - Details on the exams
- Course content - R
  - An overview of the content we will cover in the course

Topics, contd.

- Cyber world actors - R

  Highlights on some of the most important participants in the cyber world

- The realities of the cyber world - R

  Some interesting observations on the realities of the cyber world and its interaction with the "real" world

Topics, contd.

- CSCI e45b recap - O

  A run through all the modules of e45b, for those who were and were not there

Image credits

All drawings and photos by Scott Bradner or Ben Gaucherin unless noted

Slide#	credit
4	Cartoon of Scott from the Boston Globe
4	Cartoon version of Ben from madmenyourself.com
4	DCE shield
5	http://sweetclipart.com/theater-masks-silhouette-908
5	https://www.pinterest.com/pin/145100419217897323/

Introduction

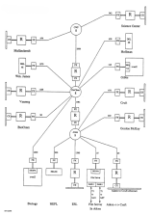
Scott Bradner

CSCI E 45: The Cyber World

Scott Bradner

- Retired in late 2016 from Harvard Office of the University CTO
- Senior Technical Consultant
- ~25 in Harvard central IT
- ~25 years at Harvard Psychology Department
- Created and managed Network Device Test Lab

Scott Bradner, networking



- Installed Harvard's first inter-building data network
- Harvard's initial ARPANET & NSFNet technical contact
- Co-founded NEARnet
  - New England Regional Data NETwork
  - Chair of NEARnet technical committee

Scott Bradner, IETF

- Involved in IETF between 1989 and 2016
- Started attending in 1990
- Co-director of multiple areas
  - Operational Requirements
  - IP Next Generation
  - Transport
  - Sub-IP
- On IESG for 10 years
- Authored 43 RFCs
- Chaired 7 working groups

Scott Bradner, teaching

- Senior preceptor – Computers in Psychology for ~8 years
- Instructor – Networld+Interop & private classes
- Instructor – Harvard Extension school since 1995
  - Petra T. Shattuck Excellence in Teaching Award

Scott Bradner, other

- Consultant, expert witness in Communications Decency Act, Wikimedia v NSA, and patent cases
- Harvard's ARPANET & NSFNET technical contacts
- Active as part of the "first wave" of the Internet

  Got my first email address in about 1972

sob@harv10
sob@harvard.edu
*!genrad!wjh12!sob

Image credits

Drawings by Scott Bradner unless noted

Slide#	credit
2	Boston Globe
4	IETF logo - https://www.ietf.org/logo/
5	Harvard Shield
	Networld + Interop logo
	Harvard extension school logo
6	supreme court logo
	ARPANET MAP

Introduction

Ben Gaucherin

CSCI E 45: The Cyber World

Ben

- CIO for Harvard Campus Services
- Formerly
  - Deputy CIO for Harvard University
  - CIO & CTO for Harvard Law School
- Participate in other people's courses
  - CS50 Hack-a-thon and seminars
  - IGA 236M Technology, Security, and Conflict in the Cyber Age, etc.

Ben, contd.

Sapient

- Many years with Sapient Corp.
  - CTO for the last 6 years
  - Involved in many major business transformations
  - Across many industries: federal government, energy services, financial services, casino, retail, telecommunication, etc.
  - Building lots of large/complex systems, leveraging a wide variety of technologies

Ben, contd.

- Senior advisor to technology companies, and consultant/expert witness on large global technology litigation cases
- And a few other things:
  HR software product, French Air Force, nuclear research center, Ad agency, coal mines, etc.

Ben, contd.

- Academics:
  "Maîtrise" in Computer Science and Mathematics, "Brevet de Technicien Supérieur" (BTS) in Electrical Engineering
- Early form of "digital native"*
- Active in the "second wave" of the Internet

* *Digital Natives, Digital Immigrants* - Mark Prensky - 2001

Image credits

All drawings and photos by Ben Gaucherin unless noted

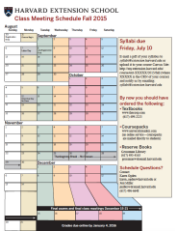
Slide#	credit
2	Cartoon version of Ben from madmenyourself.com
3	Sapient logo
4	HayGroup, Trolex ltd., GANIL, and French Air Force logos
5	Université de caen– Fouad Giri - https://giri.users.greyc.fr/images/stories/atout3_01.JPG
5	"Minitel1980" by Jef Poskanzer Uploader: Joho345 - Flickr http://www.flickr.com/photos/jef/320700986/. Licensed under GFDL via Wikimedia Commons - https://commons.wikimedia.org/wiki/File:Minitel1980.jpg#/media/File:Minitel1980.jpg

Introduction

Course logistics

CSCI E 45a: The Cyber World – part A

Course structure



- Runs over 14 weeks
- One or more modules posted per week (on Sunday mornings)
  - No posting during vacation
- The modules were taped between 2015 and 2016
- But the world changes continuously, so we post updates when necessary

Course structure, contd.

- Each module includes multiple topics
- Most topics are "required"
  - i.e. they are included in the exams
- Some are optional

Teaching Assistants (TAs)

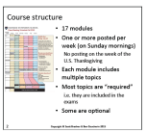
- We have a number of Teaching Assistants who …
  - Are here to help you and answer questions you might have about the course
  - Help prepare and grade the exams
  - See the list of TAs on the course website

Contacting us

- We have a teaching staff email list that includes both instructors and the TAs e45a@sobco.com to be used for:
  - Any question about the course
  - Requests for grading reconsideration
  - Letting us know of interesting world events relating to the course

ALWAYS USE THIS ADDRESS – DO NOT use Canvas to communicate with us

Slides & handouts



- Slides comprise talking points
- Not sufficient by themselves
- Illustrations on the slides attempt to be relevant but are for visual effect not content
- PDF of the handouts posted along with videos
  - For use only with the class, please do not reproduce for other uses – **school rules!!**

Reading


Dr. Betsy Sparrowr


Jenny Liu


Daniel Wegner

- Lots (and lots) of reading
- By design, lots of reading - comes with the territory
- We do not expect you to actually read every word
- We want you to learn how to "read smart"
- Get the gist of the reference and understand where to find the information later

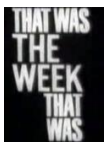
7

Check Your Understanding quizzes

- Short quizzes in some modules
- Meant to help you validate that you understand the material in the module
- Optional
- Do not factor in the course grade

8

Discussions



- Click on Discussion to find discussion topics
  - Module discussions
  - "News you can use" discussions
  - Other topic discussions
- Your participation is not monitored or graded but you may find it useful

9

Other things you should know…

Chaucer – Canterbury Tales

- English
  - All readings are in English
- How to use the Internet
  - All readings are on-line
- The basic structure of the U.S. legal system
  - Unless stated otherwise, exam questions are to be viewed in the U.S. legal context

10

News You Can Use (NYCU)

- Each week will include "News You Can Use"
- We will report on news items involving Internet technology, security, policy issues or developments to tie the course to current events
- We expect you to follow-up and find out more about these issues

11

News You Can Use (NYCU), contd.

- News topics not included in the handouts
- Separate list of article titles posted in an on-line Discussion
  - URLs not posted because we want you to look around at other coverage
- The news topics are part of the course and therefore will be part of the exams
- Please send interesting ones to the teaching staff email list

12

News you can use – Follow Bruce!

- https://www.schneier.com/
- Special case
  - Publishes relevant material regular basis
- Some of his postings will be on the exams
  - Postings from the first day of the semester through the opening of the last exam are in-scope for exams. Questions will be on Bruce's own words in his blog, not articles he links to (including his own articles)

Image credits

All photos by Scott Bradner unless noted

Slide#	credit
2-3	Harvard Extension School calendar
4	http://www.keepcalm-o-matic.co.uk/p/keep-calm-i-m-a-teaching-assistant/
5	Bradner: Boston Globe
	Gaucjerin: from madmenyourself.com
7	Sparrow: http://www.yalescientific.org/2013/05/is-google-ruining-your-memory-the-science-of-memory-in-the-digital-age/
	Liu: https://ca.linkedin.com/in/liujenny23
	Wegner: http://www.psychologicalscience.org/index.php/members/awards-and-honors/fellow-award/recipent-past-award-winners/wegner
8	http://fcpspart1dentistry.com/quiz-of-dental-materials-1/
9	https://www.youtube.com/watch?v=6NtmGlvHbqA

Introduction
Exams

CSCI E 45a: The Cyber World – part A

Exams and grading

Open 9AM to 9AM a week later

- 4 exams
  - Take on-line at-home, open book/Internet
    - 25 questions each, 4 points max per question
  - Exams are **cumulative**
  - Exams open at 9 AM on a Wednesday and close at 9 AM the following Wednesday
  - You must complete the exam within 5 days of opening it or by the end of the window whichever comes first
  - Verify that you will have time to do the exams or please drop the course

Exams and grading, contd.

- Read exam questions carefully as some of them ~~may~~ will be misleading
- By "misleading" we mean "carefully worded"
  - e.g., might ask *how does x do y* when x does not do y
- The course topics involve precision
  - You need to know just what problem you are trying to solve and be able to say clearly what the solution is

Exams and grading, contd.

- The real world does not present clear questions, neither do we
- We use the exams to see if you understand & can explain the material
- Answer the exam questions as you would answer technical questions from your boss
  - Clear and to the point

Exams and grading, contd.

- Hints
  - If the question includes "true or false?" your answer needs to have the word "true" or the word "false" in it for full credit
  - If the answer to the question is "ICMP" then "ICMP" or "Internet Control Message Protocol" must be in your answer.
  - If the question has two parts, so must your answer
  - Think about why we asked the question – what did we want to know?

Exams and grading, contd.

- Extraneous information
  - Unless the question asked you to explain ICMP, any explanation of ICMP will be "extraneous information"
    - One student provided a 320 word answer where "ICMP" was enough
  - Extraneous information makes it hard to tell if you know what you are talking about
  - One point will be taken off for any extraneous information
    - E.g., how TCP works, how the IETF makes standards, vulnerabilities in a protocol … unless the question asks for it

Exams and grading, contd.

- i.e., answer the **actual question that was asked and only answer that question**
  - Most questions can be answered in less than a dozen words – many in one or two words
- Goldilocks principle applies to your answers - **your answers should be as short as they can be without missing any key points**
- By the way, there is no need to repeat the question in the answer

Exams and grading, contd.

- The answers to all questions can be found in the lectures or reading (including NYCU)
  - Google (or Bing) does not rule
- essay question concurrent with the last exam
  - essay optional for undergraduates
  - essay mandatory for graduates
  - grade: 0-5 points

course grade
undergraduates = ((e1 + e2 + e3 + e4)/4) + essay
graduates = (((e1 + e2 + e3 + e4)/4) *.95) + essay

Grade Mapping

A:	93-100
A-:	90-92
B+:	87-89
B:	83-86
B-:	80-82
C+:	77-79
C:	73-76
C-:	70-72
D+:	67-69
D:	63-66
D-:	60-62
E:	0-59

- scores are mapped into grades only at the end of the semester, and then only after any optional essay score is added as well as any possible curve
- fractional values rounded up
  - 92.4999 = 92
  - 92.5 = 93

Exams and grading, contd.

- Give **proper attribution** to any supporting citations
- Answers have to be in **your own words**
- Be smart!
  Individual not collaborative effort
- We are **required** to report potential plagiarism & collaboration to DCE

9

Use Your Own Words!

Use your own words!

(If more than ~5 words)
Do not just cut & paste
We want to know if you understand

9A

Sample question #1

- Pirate Jill, who lives in the U.S., likes to download movies from her favorite torrent site. Due to lawsuits, the site will no longer service any host with a US IP address. Without moving out of the country, how can Jill continue to access this site?
- Use a VPN with server located outside the US
- Use a proxy located outside the US

10

Sample question #2

- Does a TCP acknowledgment guarantee that data has been received by the end user? Briefly explain.
- No, only that the receiving node's TCP stack has assumed the responsibility to deliver it.

The making of exam questions

- Try to test understanding of concepts
- Try to test thinking not just fact recall (but some fact recall)
- Answer not Googleable
- Test ability to see details (e.g., in the question itself)

  Note – if you have a hard time breaking a problem into logical parts you will not do well in this field

PS

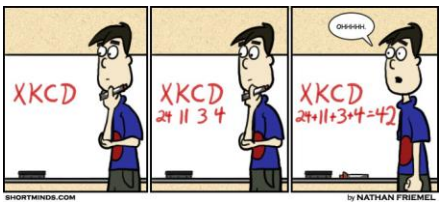


Image credits

Slide#	credit
2	http://firearmsafetycanada.com/?page_id=12
3	http://ecatalog.mitutoyo.com/Micrometers-C1066.aspx
4	http://4suitcases.com/2010/05/what-exactly-is-the-real-world/
5	https://www.youtube.com/watch?v=-5Jy0mn2M4c
5A	https://worldartsme.com
6	http://slideplayer.com/slide/10716853/ slide 5
7	https://cottagedoorpress.com/products/goldilocks-and-the-three-bears-board-book
8	http://humancapitalist.com/is-open-book-management-a-good-fit-for-your-company/
9	https://www.pantone.com/pci/minion-yellow?from=hp
10	https://geology.com/world/world-map.shtml
11	http://clipart-library.com/man-computer-cliparts.html
12	http://www.principalspage.com/theblog/archives/you-need-more-than-the-ability-to-take-tests
13	https://knowyourmeme.com/photos/313299-the-answer-to-life-the-universe-and-everything

16

Introduction
Course content

CSCI E 45a: The Cyber World – part A

Course origins

- Initially two courses taught by Scott:
  - E132 – Advanced topics in Data Networking Protocols and Network Architectures
  - E170 – Security, Privacy and Usability
- Scope now entire "cyber world"
- Updating old content and adding new content
  - Hardware, Software

Who is this course for?

- Attempting to address a growing need/demand
  - No longer sufficient to be a "good computer user"
- Targeted at geeks, lawyers and other curious minds
- People who want to understand:
  - The technologies involved
  - Important ideas and concepts behind the technologies
  - Laws, policies, information security, etc.

What this course is about

- Understanding of how the technical and policy elements of the cyber world work
- Promote critical thinking
- Promote multi-faceted views/approaches
- Learn from failure

"There is no success like failure, and failure is no success at all"
Bob Dylan: *Love Minus Zero/No Limit*

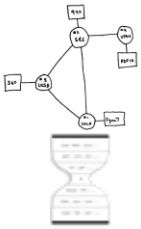
4

What this course is NOT

- A detailed technology practitioner's course
  - You don't need to be an engineer
  - And it's definitely fine if you are one
  - And it's okay if you don't want to become one
- In-depth in any one area – you won't become a topic expert from this course

5

Overview of the modules



- Digital technology and computing devices
  - From bits to bytes, and how a generic computing device works
- History of the Internet and concepts
  - Key ideas and people that led us to the Internet of today
- Internet protocols
  - IP, TPC, UDP, etc. the "dial tone" of the Internet

6

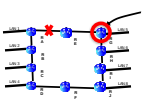
Overview of the modules, contd.



- Software – simple software
  - Making, running, and abusing software
- Network technologies
  - Layer 2 & 3 technologies, SDN, MPLS, etc.
- Designing and building the infrastructure
  - From the network jack to the large scale ISP

Overview of the modules, contd.





- Software – distributed systems
  - Composing simple software into bigger systems
- Middleware
  - The essential, and (sometimes) transparent things in the network that make it work
- Routing
  - How do packets get from one end of the globe to the other, or to the computer down the hall

Overview of the modules, contd.


- The cloud
  - Beyond the hype, what is it and how to think about it
- Managing the infrastructure
  - When you are in charge of a large infrastructure, how do you manage it?
- Security fundamentals
  - From Confidentiality, Integrity, Availability to encryption, and digital trust systems

Overview of the modules, contd.

- Security tools
  A walkthrough the landscape of security tools
- Internet regulation & governance
  From the regulation of telephone networks, to the current messy landscape of Internet governance
- Technology standards
  How do technology standards get developed, contrast and compare between ITU and IETF

Image credits

All drawings and photos by Scott Bradner unless noted

Slide#	credit
2	Harvard Extension School shield
3	channel4.com
4	www.musee-rodin.fr
5	https://ia802505.us.archive.org/zipview.php?zip=/33/items/olcovers6/olcovers6-L.zip&file=61922-L.jpg

Introduction
Cyber world actors

CSCI E 45a: The Cyber World – part A

Individuals

- You as an individual
  - As a person
  - Independently from any organization affiliation
- Other individuals (activists)
  - Disclosers/Whistleblowers
  - Hackers (white and black hat)
  - Crooks
  - Idealists

Governments

- National security
- Law enforcement
- National infrastructures
- Social order
- Technology governance
- International issues
  - espionage, cyber conflict

- Provide services to citizens
- Collect large volumes of data

Internet Service Providers (ISPs)

- Providers of Internet connectivity
- Some publically traded, some privately owned
- Increasingly concentrated
- Primary focus is on revenue and profit

4

ISPs, contd.

- Are increasingly The communications infrastructure
- Often a relationship of convenience with governments

5

Technology providers

Google

Microsoft

- Hardware, Software, etc.
- Primary focus is on revenue and profit
- Often a relationship of convenience with governments
- What's really in the box?
  Un-documented "bits" and "hooks"

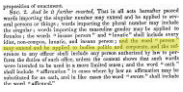
6

Other businesses, commercial entities

amazon.com

- Users of the Internet
- "Stuff" sellers, content sellers/providers, advertisers
- Primary focus is on revenue and profit
- Often a relationship of convenience with governments
  - e.g., data to NSA from Microsoft, Google, …
- Collect a lot of data about everyone "who comes in contact"

Natural Persons vs. Artificial Persons



1871 version

- Corporations are often treated as people in US law
  - *In determining the meaning of any Act of Congress, unless the context indicates otherwise …*
  - *the words "person" and "whoever" include corporations, companies, associations, firms, partnerships, societies, and joint stock companies, as well as individuals*
  - US Code, Title 1, Chapter 1, Section 1

Corporations as Persons

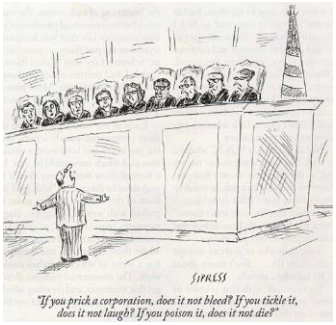
DARTMOUTH
VOX CLAMANTIS IN DESERTO
1769

CITIZENS UNITED

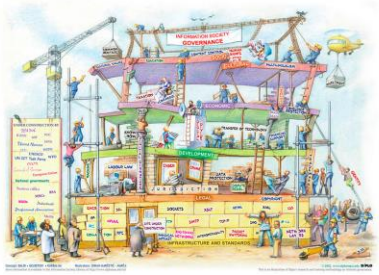
HOBBY LOBBY

- 1st case: corporations can enter into contracts
  - Dartmouth College v. Woodward 1918
- More recent cases: corporations have first amendment rights
  - Citizens United v. Federal Election Commission 2010
  - Burwell v. Hobby Lobby 2014

Corporations as Persons



Information society governance



Non Government Organizations (NGOs)

- Internet Corporation for Assigned Names and Numbers (ICANN)
- Internet Governance Forum (IGF)
- Internet Society (ISOC)
- Number Resource Organization & Regional Internet Registries (RIRs)

Regulators

- U.S.
  - Federal Communications Commission (FCC)
  - Individual states' Public Utility Commissions (PUCs)

- France
  - Autorite de Regulation des Communications Electroniques et des Postes (ARCEP)

- International
  - International Telecommunications Union (ITU/UN)
  - World Intellectual Property Organization (WIPO)

Standards Development Organizations

- International Telecommunications Union (ITU)

- Internet Engineering Task Force (IETF)

- European Telecommunications Standards Institute (ETSI)

- Worldwide Web Consortium (W3C)

- International Organization for Standardization (ISO)

SDOs, contd.

- American National Standards Institute (ANSI)

- Institute of Electrical and Electronics Engineers (IEEE)

Notable non-profit

- Electronic Frontier Foundation (EFF)
- Center for Democracy and Technology (CDT)
- The Heritage Foundation
- European Digital Rights (EDRI)
- Association Electronique Libre (AEL)
- Bits of Freedom (BoF)

... and many more

16

Image credits

All drawings and photos by Scott Bradner unless noted

Slide#	credit
2	blackhat logo
	E Snowden photo
3	logos - http://en.wikipedia.org/wiki/File:US_Intelligence_Community_members.gif
4	isps - http://www.redcondor.com/solutions/success-stories.htm
5	isps http://www.redcondor.com/solutions/success-stories.htm
6	internet in a box - http://encosia.com/6953-reasons-why-i-still-let-google-host-jquery-for-me/
	apple logo
	google logo
	microsoft logo
7	amazon logo

17

Image credits

All drawings and photos by Scott Bradner unless noted

Slide#	credit
8	http://www.english.illinois.edu/-people-/faculty/debaron/584/584reading/01dictionaries.pdf
9	Dartmouth shield
	Citizens United logo
	Hobby Lobby logo
10	The New Yorker Mar. 14, 2011
11	http://www.diplomacy.edu
12	ICANN logo
	IGF logo
	Internet Society logo
	NRO logo

18

Image credits

All drawings and photos by Scott Bradner unless noted

Slide#	credit
13	FCC logo
	ARCEP logo
	ITU logo
	WIPO logo
14	ITU logo
	IETF logo
	ETSI logo
	W3C logo
	ISOC logo

19

Image credits

All drawings and photos by Scott Bradner unless noted

Slide#	credit
15	ANSI logo
	IEEE logo
16	EFF logo
	CDT logo
	Heritage Foundation logo
	ERDi logo
	AEL logo
	Bits of Freedom logo

20

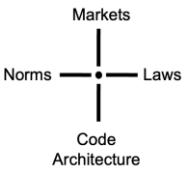
Introduction

The realities of the cyber world

CSCI E 45a: The Cyber World – part A

1

The Lessig model



- The laws of cyberspace
  - Essay written by Larry Lessig
  - Aimed at debunking early days hype about cyberspace
    - *"[cyberspace] has the potential to be the antithesis of a space of freedom."* (1998)
  - Points out the four forces regulating behavior in cyberspace
  - Contrasts real world regulations to regulations in cyberspace

2

Impacts and responses

- Let's look at a collection of factoids to understand
  - The dynamic of things in the cyber world
  - Interactions with the "real" world
  - Society
  - Business
  - Etc.

3

States


Moxie Marlinspike

- Difference between totalitarian regime and social democracy—harder to figure out
- The "nanny state"
  - Protecting you from all the bad things you could be exposed to
- The "security state"
  - Protecting the state from you

4

Freedom and oppression

- Hacktivists
  - Egotistical view of what is important
- The Internet, for freedom and oppression
  - Effective tool for dissenters
  - Effective tool for governments to track "trouble makers"

5

The business of data and information

- Ever larger commercial entities:
  - Running large portions of global infrastructures
  - Amassing large amounts of information on everyone
  - Benefiting from cyber-espionage
    - Governmental and private

6

Business challenges & emerging responses

- Difficulty in mapping real world constructs to the cyber world: legal jurisdiction, taxation, trademarks, etc.
- Virtual currencies threatening old economies
- Development of "darknets" and the crime "service sector"

7

Law Enforcement/Counter-terrorism

- Abilities they never had before
- Total information awareness
  - Traditional government view: the more information you have the safer you are
- Worried about the bad guys "going dark"
  - Crypto-wars still going strong
- Ability to bypass national legal frameworks through multi-national agreements

8

Regulatory power plays

- Nations still think in nationalistic terms
  - Regulations to protect the nation state
  - International covert collaboration rising
- Myopic industry groups
  - One's industry should dictate/constrain priority and fundamental architecture elements of the Internet

9

Underlying tussles

- "Bell Heads" vs. "Net Heads"
- Net neutrality
- Social norms and culture clashes
- Cyber conflicts
- Data accessibility v. privacy

10

Image credits

All drawings and photos by Scott Bradner unless noted

Slide#	credit
2	Larry Lessig – austinchronicle.com
5	Photo by Adam Berry - http://www.slate.com/content/dam/slate/articles/health_and_science/future_tense/2012/04/120419_FUTTENS_GuyFawkesProtester-EX.jpg.CROP.rectangle2-mediumsmall.jpg
6	http://lordheath.com/index.php?p=1_135_big-business
9	United-academics.org http://www.united-academics.org/magazine/design-technology/hats-from-history/

11

Introduction

E45b review

CSCI E 45a: The Cyber World – part A

What you should remember from the second semester, even if you haven't been there yet

This is an overview of the terminology and concepts covered in the second semester – this material will not be included in the exams except where explicitly covered in this semester

E45b Review: Internet governance

Internet governance

- Many issues influence Internet governance
- Jurisdictional disconnect
  - Network and legal boundaries different
- Trademark global rather than local
- Copyright holders trying to figure out a profit mechanism

E45b Review: Internet governance

- State security
  - Protect the government from disruption
- Cyber attackers
- Support for emergency use
- ISP business model
  - Do they need a piece of the action?
- Privacy
  - From governments, from companies
- Technology constraints on lawmakers

E45b Review: Internet governance

- Morality
  - Governments know what is good for you (better than you do)
- Players
  - Regulators, cops, SDOs
- Legal concepts
  - Openists v Deregulationists
  - Network neutrality
- Some US laws
- International pressure

regulation of the Internet is a "moral imperative"

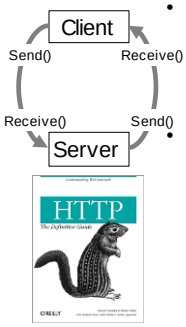
E45b Review: Internet application protocols


DIALOGO
DI
GALILEO GALILEI LINCEO
MATEMATICO SOPRAORDINARIO
DELLO STVDIO DI PISA.
E Filosofo, e Matematico primario del
SERENISSIMO
GR. DVCA DI TOSCANA.
Doue ne i congressi di quattro giornate si discorre
sopra i due
MASSIMI SISTEMI DEL MONDO
TOLEMAICO, & COPERNICANO,
Proponendo indeterminatamente le ragioni Filosofiche, e Naturali
tanto per l'vna, quanto per l'altra parte.
CON PRI VILEGI.
IN FIORENZA, Per Gio: Batista Landini MDCXXXII.
CON LICENZA DE' SVPERIORI.

Internet application protocols

- Internet applications listen on a network port and expect a specific protocol
- Protocol:
  - Structures, and sequence of network messages required to implement an application
  - Methods, Header fields, and Error codes
  - Most IETF protocols plain text

E45b Review: Internet application protocols



- Client/server
  - Client – the machine/software from which requests originate
  - Server – the machine/software fulfilling the request
  - System can be both
- Examples:
  - Finger – get status of users on another system
  - SMTP – email exchange
  - HTTP – web data transfer
    - Can use "cookie" for state information
  - SIP – Voice over IP
  - SSH – remote login & tunneling

E45b Review: Identity and authentication

123-45-6789

Identity and authentication

- An identity
  - Uniquely specify an individual person - e.g., SSN
- Authentication
  - Bind a physical person to an identity
  - Done with an authenticator
    - Know – e.g. password, SSN
      - Lots of problems
    - Have – ID card, smartphone
    - Are – fingerprint
    - Can do - signature

E45b Review: Trust and privacy

Trust and privacy

- Trust:
  - Belief in the predictability of behaviors and outcomes within a given scope of activity
- Trust and the Internet:
  - Essential for people to do things online
  - Internet magnifies real world's abuses of trust
  - Many point solutions to trust on the Internet
  - But, no general solution to trust on the Internet

E45b Review: Trust and privacy


Samuel Warren


Louis Brandeis


Justice William O Douglas

constitutional right to privacy under threat

- Privacy:
  - The ability to keep your personal information from being known by others
  - Not same as anonymity
- Limited right to privacy read into U.S. Constitution
  - Privacy not explicitly mentioned in the constitution – penumbra right
  - "zone of privacy" in areas of making decisions and keeping personal matters confidential
- Katz v U.S. key case for privacy:
  - Privacy only where there is a "reasonable assumption"

10

E45b Review: Trust and privacy

- Different approaches
  - E.U. – principle-based related to use of data
  - U.S. – point solutions driven by events
- E.U. and California trend setters
- U.S. laws and privacy:
  - Freedom from disclosure
  - Laws requiring disclosure of private information
  - Freedom from nuisance

11

E45b Review: Security threats

Security threats I

- Malware: software that does things the user does not expect
  - *Includes worms, viruses, spyware, Trojan horses, adware, and other software that installs programs without user knowledge* www.stopbadware.org
- Functions
  - Propagate virus
  - Adware
  - Ransomware
  - Backdoor/RAT
  - Spyware

12

E45b Review: Security threats

- Mechanisms:
  - Worm - Autonomous propagation technical attack
  - Virus - Requires user action to propagate – social attack
  - Trojan – malware hidden in legit program
- Other threats
  - Network monitoring
  - Man in the Middle
  - DoS, DDoS
  - Buggy software

13

E45b Review: Security threats

Security threats II

- Attacks on websites
  - Defacement
  - Data stealing, causing actions
    - SQL injection, cross-site scripting
  - Browsers are attack facilitators
    - E.g., Flash Player

- Social engineering
  - Hacking wetware (people)
    - Crimes of persuasion
  - Can not be stopped by technology alone

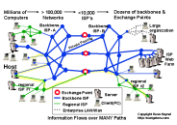
14

E45b Review: Security threats

- Facilitators
  - People do not fully appreciate the importance of security controls and their role in following them
- General types:
  - People acting "normal"
    - Normal for the situation
    - Are often not verified
  - Believable communications
    - Correspondence that "looks right"
    - E.g. phishing
- Hard to protect against
  - Paranoia useful, as are clear policies & management support

15

E45b Review: Protecting the infrastructure



Protecting the infrastructure

- Threats via the Internet
  - Espionage, theft, disruption & extortion
  - Generally, protection is end site responsibility
  - Ad-hoc approach, few regulations
- Threats to the Internet
  - Attack core services (e.g. DNS & routing) or devices (e.g., routers)
  - Physical layer generally redundant and resilient
    - Fibers, etc.
  - Ad-hoc approach, few regulations
    - Blocked by politics

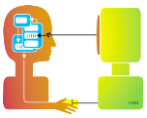
E45b Review: Protecting the infrastructure

YouTube

SIDR

- DoS & DDoS
  - Overload link or service
  - DNS servers can be protected against DoS with anycast
- Protecting routing
  - For misrouting, technology available, little deployment
    - Only protects against some threats
- Protecting against DNS corruption
  - Technology available, some deployment

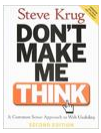
E45b Review: Usability accessibility



Usability accessibility

- Human Computer Interaction
  - Study of interaction between people and computers
- Not just about pretty colors and fonts
- "user friendly" is context dependent
- Overall process
  - Discover, Design, Evaluate
- Complex process
  - User's mental model of tasks, cultural norms, function over form, etc.

E45b Review: Usability accessibility



- Different ways to discover
  - Focus groups - asking users/customers what they want
  - Ethnography – observing people performing the work/task
  - Let users hack the product
  - Or rely on superior design beings
- Usability principles
  - Don't frustrate the user
  - Learnability, Flexibility, Robustness
- The human body is a "human processor", with an interface with its own limitation

E45b Review: Usability accessibility

- Security often in conflict with usability
- Accessibility:
  - Need to make cyber accessible to all
  - As it pertains to the American with Disability Act (ADA), web sites considered places of public accommodation
  - W3C's Web Accessibility Content Guidelines (WCAG) 2.0 is the prevalent standard for accessibility

E45b Review: Cyber conflict

Cyber conflict

- War: A contention by force; or the art of paralyzing the forces of an enemy to achieve strategic objectives
- Laws of war:
  - jus ad bellum – "justice to war"
  - jus in bello – "justice in war"
  - In the U.S.
    - DoD directive 5100.77, USC Title 10, USC Title 50
- Sherman's "scorched earth" policy
  - Paralyze the enemy by destroying their infrastructure

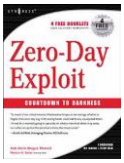
E45b Review: Cyber conflict

- Traditional doctrine, concepts of conflict/war do not map well to cyber
  - Internet mostly ignores national borders
  - Attribution near impossible
  - Arms control near impossible
  - Conflict management made difficult
- Cyber weapons can kill or incapacitate
  - Industrial Control Systems, life safety control systems, AI controlled weapons systems

E45b Review: Cyber conflict

- Actors:
  - Governments, businesses, crime, individuals
- Different activities:
  - Cyber crime
  - Hacktivism
  - Cyber exploitation
  - Cyber attacks
- Multiple cyber conflicts
  - But is cyberwar war?

E45b Review: Cyber conflict




Ryan Ellis

- Zero days:
  - Unpatched exploit
  - Product of humans writing software
- Market for zero days
  - Unregulated, black market, like drug deals
- Disclosure models
  - Limited: disclose to vendor
  - Full: disclose to force a patch
  - Coordinated: tell vendor first
  - No disclosure: sell vulnerability

E45b Review: Commerce DRM

Commerce DRM

- E-commerce
  - B2B half or more of total
  - B2C: small but growing segment
- Payment systems for B2C
  - Card-based: credit & debit cards
    - Card present mode
      - Token (card) based authentication
    - Card not present mode
      - Knowledge based authentication
    - Employ anti-fraud techniques
  - Non-card systems
    - Apple, Android & Samsung pay
      - Tokenized – merchant does not get card number - safer

E45b Review: Commerce DRM

© May 21, 1928

- Copyright
  - Author/creator can control use "for a limited time"
  - Many special case in laws
    - E.g. first sale, fair use
- All works automatically copyrighted when created
- Length of protection varies between countries
  - U.S. life of author + 70 years
- Digital world has made copyright much harder
  - E.g., copies are perfect

E45b Review: Commerce DRM

- DMCA
  - Digital Millennium Copyright Act
  - U.S law concerning copyright
  - Blocks circumvention of copyright protection systems
    - With some exceptions
  - Requires service providers to respond to take down notices
- DRM
  - Digital Rights Management
  - Copyright protection systems
    - Limit user's use of copyright materials
  - Many problems
  - Some systems really dumb

E45b Review: InfoSec management mindset

Information Security Management and mindset

- Information security strategy
  - Where we are going
  - Why we are going there
  - How to get there
- Data classification
  - Part of risk assessment

- Policies
  - Rules to guide decisions and actions
  - Laws: government policies

E45b Review: InfoSec management mindset

- Policies come from
  - Explicit policy development process
  - Dealing with the un-expected
  - Implied policies
  - Externally imposed
    - Laws, regulations & contracts
- Good policies
  - Goldilocks principle – just right
  - MUST, MUST NOT, SHOULD, and SHOULD NOT
  - Few exceptions
  - Not technology specific
  - Clear, practical & actionable
  - Periodic & after incident reviews

E45b Review: InfoSec management mindset

- Information security program
  - Owned and led by CEO, managed by CISO
  - Includes:
    - Governance & compliance
    - Standard operating procedures
    - Designated security staff
    - Communication & awareness program
    - On-going assessment process
    - Implementation of controls
  - Get users to be part of program & be accountable

E45b Review: InfoSec management mindset

- Security mindset
  - *"Being security conscious means being a criminal, if only in one's head"*
  - Always thinking of ways to subvert the systems
  - Must understand risk
- Hackers
  - Creative engineering minds
  - Ability to un-learn, do away with assumptions
  - Appearances may be misleading

E45b Review: Surveillance

Surveillance counter-surveillance

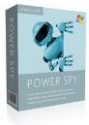
- Governments & private sector
  - NSA: dual mission
  - Google: to serve "better" ads
  - Employers: employees as chattel
- Surveillance much easier in digital world
- Legal limits being developed

E45b Review: Surveillance

- Multiple laws enabling and protecting from surveillance
  - CALEA, National Security Letters, U.S. Wiretap Act, Electronic Communications Privacy Act, …
- Techniques
  - Evesdropping & emmissions monitoring
    - TEMPEST emissions reduction
- NSA
  - Snowden revelations showed how extensive NSA surveillance was
  - Broad brush rather than targeted

Edward Snowden

E45b Review: Surveillance



- Non-government surveillance
  - Ad companies & ISPs to pay for a "free" Internet
    - Try to understand Internet users to feed them "better" ads
- Employers
  - No constitutional protection
    - Can spy on any activity
    - As long as it is not upon request of the government
- Pervasive surveillance changes society
  - By definition

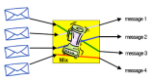
E45b Review: Surveillance

- Anonymity
  - Good and bad people need it
  - Protected for political discussions by U.S. Constitution
  - Outlawing anonymity would change things only for honest people
- Privacy protecting technology
  - Encryption – scramble content
  - Steganography – hide content
  - Device-based
    - Mixers, proxies, onion routing

E45b Review: Surveillance

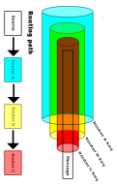
- Encryption
  - The most commonly used encryption good for government top secret communications
  - Encryption not weak point, key handling / end system security are
  - Encryption does not hide who is communicating & can show you have something to hide
  - IETF & others are pushing "Opportunistic encryption" – encrypt all the time so important stuff does not stand out

E45b Review: Surveillance



- Mixer
  - Decrypts/encrypts/permutes messages sent through it
  - Hides who is talking with who
- Proxies
  - Forward traffic through proxy
  - Encrypted connections to and from
  - Traffic looks like destination/source is the proxy
  - Can bypass firewalls

E45b Review: Surveillance



- Onion routing: secret communication
  - Pass messages through random set of relays using layers of encryption, each hop decrypts & forwards message
    - Inside: end-to-end
    - Next: end to last hop
    - Next: end to next to last hop
    - ...
    - Next: end to first hop
- Tor: The Onion Router
  - > 1K relays across Internet
  - Original funding: U.S. Navy

E45b Review: Safe computing

Safe computing

- For enterprises
  - Protecting key data assets, and technologies essential to business operations
  - Few useful standards that provide explicit, detailed guidance
  - PCI-DSS useful outside of credit card business
  - Standards are not a protection against stupidity, or an excuse not to think

E45b Review: Safe computing

- For individuals
  - Don't get phished (or more generally fooled)
    - Think before you act
  - Think about the future
    - Should you be posting this?
    - Should you be going to this sort of site?
  - Stay informed
    - Rules change.
    - What was ok yesterday may not be today

E45b Review: Safe computing

- For people, contd.
  - Practice good hygiene
    - Should you be plugging this in your computer? Should you be clicking on this?
  - It's 10:00 pm, do you know where your data is?
    - Be a good information steward: encrypt, erase securely when disposing of a computing device

Image credits

Slide#	credit
3	derby – http://store.kentuckyderby.com/kentucky-derby-merchandise.php
	Olympic logo - http://www.rampantscotland.com/know/blknow_olympics.htm
4	http://www.freerepublic.com/focus/news/3272638/posts
	http://www.thevaunter.com/tfl/google-and-facebook-privacy/c16tv
5	FCC - https://www.fcc.gov/logos
	http://www.itu.int/en/history/Pages/ITULogo.aspx
	http://www.thestar.com/news/world/2013/03/06/is_nicolas_sarkozy_about_to_make_a_comeback.html
6	https://writinglabatunt.wordpress.com/2015/02/22/galileos-dialogue-sparks-controversy/
8	http://akamaicovers.oreilly.com/images/9781565925090/cat.gif
9	https://www.flickr.com/photos/metropolismusic/2667617635
	rsa https://commons.wikimedia.org/wiki/File:RSA_SecurID_Token_Old.jpg
	eye https://scienceeasylearning.wordpress.com/page/9/
	signature https://commons.wikimedia.org/wiki/File:Elvispresley-logo.svg
10	http://www.thepublicistnovel.com/wp-content/uploads/2015/01/stay-paranoid-and-trust-no-one.png
11	https://en.wikipedia.org/wiki/William_O._Douglas
12	http://www.chadsteurlaw.com/AboutUs.html
13	https://www.stopbadware.org/

Image credits

Slide#	credit
14	https://commons.wikimedia.org/wiki/File:Biohazard.svg#/media/File:Biohazard.svg
15	http://countermeasures.trendmicro.eu/royal-australian-air-force-website-defaced/
	https://www.rooksecurity.com/rook-uncut-successful-social-engineering-stories/
16	http://www.ruggedbutts.com/black-who-me-knit-long-sleeve.html
	http://www.admiralsecurity.com/services/armed-uniformed-security-officers/index.html
	http://www.dwgdistribution.com/eco
17	https://en.wikipedia.org/wiki/Nuclear_power_plant
	http://navigators.com/sessphys.html
18	https://kshitiz25.wordpress.com/2012/04/12/denialof-service-dos-attack/
	https://www.youtube.com/yt/brand/downloads.htm
	http://www.prweb.com/releases/2009/03/prweb2199054.htm
19	http://eswcornell.weebly.com/archives.html
20	http://www.nodevice.com/user_manual/apple/ipod/ipod_click_wheel_including_u2_special_edition_2040gb.html
	http://www.onlypencil.com/blog/wp-content/uploads/2014/01/eyefinal2.jpg
21, 22	https://en.wikipedia.org/wiki/War
23	http://www.eraofwisdom.org/guy-fawkes-mask-is-a-global-symbol-of-our-age-of-activism/
	https://en.wikipedia.org/wiki/Urengoy%E2%80%93Pomary%E2%80%93Uzhgorod_pipeline

Image credits

Slide#	credit
25	http://mashable.com/2010/10/28/b2b-social-media-marketing/#s07wkvKGgEqB
	http://creditcard.umwblogs.org/?attachment_id=5
26	http://disney.wikia.com/wiki/File:Steamboat_Willie_Pin.jpg
27	http://copyrightwatchers.blogspot.com/2010/02/digital-millennium-copyright-act.html
	https://techwhack.co/tag/apple-itunes-10/
28	https://www.linkedin.com/pulse/rout-planning-out-planning-strategery-reggie-legend
	http://www.writergirl.com/5-leadership-tips-from-a-public-policy-officer/
29	http://www.eremedia.com/tlnt/do-old-school-workplace-rules-and-hierarchies-still-matter/
30	https://www.flickr.com/photos/drbexl-/4414113538/in/photostream/
31	http://www.nbcnews.com/id/37021555/ns/travel-travel_tips/t/liquid-rules-so-long---/
32	https://commons.wikimedia.org/wiki/File:Google_2015_logo.svg
	https://commons.wikimedia.org/wiki/File:National_Security_Agency.svg
	http://blog.modernmechanix.com/what-happens-when-you-mail-a-letter/
33	https://www.quora.com/topic/Communications-Assistance-for-Law-Enforcement-Act-CALEA
34	https://commons.wikimedia.org/wiki/File:Google_2015_logo.svg
	https://commons.wikimedia.org/wiki/File:Verizon_logo.svg
	http://www.ematrixsoft.com/power-spy-software.php
35	http://techland.time.com/2012/05/24/the-new-york-bill-that-would-ban-anonymous-online-speech/
	http://www.themakeupgallery.info/various/tattoo/rushhour3.htm

Image credits

Slide#	credit
36	https://phpmatters.com/best-drupal-security-modules/
37	Roger Dingledine
	http://psiphon.en.uptodown.com/
38	http://ctijournal.com/what-is-onion-routing/
	https://commons.wikimedia.org/wiki/File:for-logo-2011-flat.svg