Introduction
Introduction to the introduction

CSCI E 45b: The Cyber World – part B

1   Copyright © Scott Bradner & Ben Gaucherin 2016

Welcome to
CSCI E 45b: The Cyber World – part B

Copyright © Scott Bradner & Ben Gaucherin 2016   2

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

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.

Not just security!

3   Copyright © Scott Bradner & Ben Gaucherin 2015

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

4

Copyright © Scott Bradner & Ben Gaucher in 2023

Agenda

- Scott

  A brief introduction to Scott

- Ben

  A brief introduction to Ben

- Course logistics

  All the practical details you should know about this course

- Course content

  An overview of the content we will cover in the course

5

Copyright © Scott Bradner & Ben Gaucher in 2016

Topics, contd.

RECAP

- CSCI e45a recap - O

  A run through all the modules of e45a, for those who were and were not there

6

Copyright © Scott Bradner & Ben Gaucher in 2016

Image credits

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

Slide#   credit
4   https://www.extension.harvard.edu/inside-extension/why-cybersecurity-skills-are-demand
5   Scott – Boston Globe
5   Cartoon version of Ben from madmenyourself.com
5   Harvard Extension School 2015 class schedule
5   DCE shield
6   http://www.ffwd.org/demo-day-2015-recap/

7   Copyright © Scott Bradner & Ben Gaucherin 2016

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

UPDATED

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 > 40 RFCs
- Chaired 7 working groups

UPDATED

4   © 2016 by Scott Bradner & Ben Gaucherin

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

NETWORLD +INTEROP

5   © 2016 by Scott Bradner & Ben Gaucherin

Scott Bradner, other

- Consultant, expert witness in Communications Decency Act & Wikimedia v. NSA cases, and in 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

UPDATED

6   © 2022 by Scott Bradner & Ben Gaucherin

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

7   © 2016 by Scott Bradner & Ben Gaucherin

Introduction
Ben Gaucherin

CSCI E 45b: The Cyber World – part B

Ben – at Harvard

- 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

- 11 years with Sapient Corp.
  Chief Technology Officer for 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.

Copyright © Scott Bradner & Ben Gaucherin 2016

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

Copyright © Scott Bradner & Ben Gaucherin 2016

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

4
        http://s1.reutersmedia.net/resources/r/?m=02&d=20070
917&t=2&i=1773200&w=&fh=545px&fw=&ll=&pl=&sq=&r=200
7-09-17T205833Z_01_L10398398_RTRUKOP_0_PICTURE0

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#/me
dia/File:Minitel1980.jpg

Copyright © Scott Bradner & Ben Gaucherin 2016

Introduction
Course logistics

CSCI E 45b: The Cyber World – part B

1 Copyright © Scott Bradner & Ben Gaucherin 2016

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

2 Copyright © Scott Bradner & Ben Gaucherin 2016

Course structure, contd.

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

3 Copyright © Scott Bradner & Ben Gaucherin 2016

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

4   Copyright © Scott Bradner & Ben Gaucherin 2016

Contacting us

- We have a teaching staff email list that includes both instructors and the TAs e45b@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

Use e45b@sobco.com f or ALL communication about the course – do NOT use Canv as

5   Copyright © Scott Bradner & Ben Gaucherin 2022

Slides & handouts
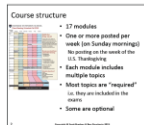
- Slides comprise talking points
- Not sufficient by themselves
- Illustrations on the slides attempt to be relevant
- PDF of the handouts posted along with videos
  - For use only with the class, please do not reproduce for other uses

no longer just a request, the school now prohibits copying

6   Copyright © Scott Bradner & Ben Gaucherin 2023

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

QQUUIZZ

- 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

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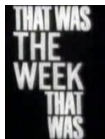
- Click on Discussion to find discussion topics
   Module discussions
   "News you can use" discussions
   Other topic discussions
- Your participation is not monitored or graded but you may find it useful

9

Other things you should know...

- 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
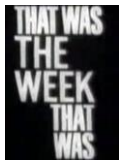 Unless stated otherwise, exam questions are to be viewed in the U.S. legal context

Chaucer – Canterbury Tales

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
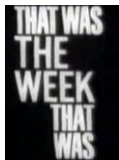- We expect you to follow-up and find out more about these issues

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

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, 11, 12 https://www.youtube.com/watch?v=6NtmGlvHbqA

10   http://www.sexualfables.com/Chaucer-and-Chaumpaigne.php

12   IETF and Apple logos

Introduction
Exams

CSCI E 45a: The Cyber World – part A

1   Copyright © Scott Bradner & Ben Gaucherin 2018-2021

Exams and grading

- 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

Open 9AM to 9AM a week later

2   Copyright © Scott Bradner & Ben Gaucherin 2018-2021

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

3   Copyright © Scott Bradner & Ben Gaucherin 2018-2021

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

4   Copyright © Scott Bradner & Ben Gaucherin 2018-2021

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?

5   Copyright © Scott Bradner & Ben Gaucherin 2018-2021

Exams and grading, contd.

obfuscation

Extraneous input causes information overload and **obfuscation**.
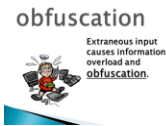
- Extraneous information
  Unless the question asked you to explain ICMP, any explanation of ICMP will be "extraneous information"
    One student provided a 320 word answer where "ICMP" was enough
  Extraneous information makes it hard to tell if you know what you are talking about
  One point will 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

6   Copyright © Scott Bradner & Ben Gaucherin 2018-2021

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

7
Copyright © Scott Bradner & Ben Gaucherin 2018 -2021

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

8
Copyright © Scott Bradner & Ben Gaucherin 2018 -2021

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

8A
Copyright © Scott Bradner & Ben Gaucherin 2018 -2021

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   Copyright © Scott Bradner & Ben Gaucherin 2018-2021

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   Copyright © Scott Bradner & Ben Gaucherin 2018-2021

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   Copyright © Scott Bradner & Ben Gaucherin 2018-2021

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.

11   Copyright © Scott Bradner & Ben Gaucherin 2018 -2021

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

12   Copyright © Scott Bradner & Ben Gaucherin 2018 -2021

PS
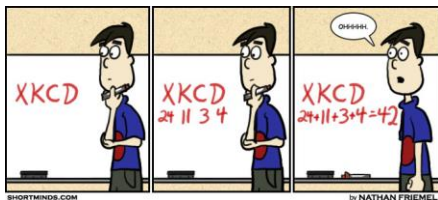
13   Copyright © Scott Bradner & Ben Gaucherin 2018 -2021

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	Copyright © Scott Bradner & Ben Gaucherin 2018-2021

Introduction
Course content

CSCI E 45b: The Cyber World – part B

1   Copyright © Scott Bradner & Ben Gaucherin 2016

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
  Security threats, cyber conflict, etc.

2   Copyright © Scott Bradner & Ben Gaucherin 2015

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.
- Now the foundation course for DCE's Cybersecurity Certificate

3   Copyright © Scott Bradner & Ben Gaucherin 2015

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
Copyright © Scott Bradner & Ben Gaucherin 2015

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
Copyright © Scott Bradner & Ben Gaucherin 2015

Overview of the modules

- Internet Governance & laws

  Who controls the Internet?

- Internet applications

  Finger, web, email, etc.

- Identity and authentication

  What is identity, and how to tie it to a person

- Trust & privacy

  Two key concepts at the center of a lot of debates

6
Copyright © Scott Bradner & Ben Gaucherin 2016

Overview of the modules, contd.

- Security threats part I & II
  Exploring digital badness
- Protecting Infrastructure
  How breakable is the Internet?
- Usability, accessibility
  The human side of technology
- Cyber conflict
  Cyber warfare, weapons, etc.
- Commerce, DRM, etc.
  The Internet as a money making platform

7 Copyright © Scott Bradner & Ben Gaucherin 2016

Overview of the modules, contd.

- Security management and mindset
  The what and how of internalizing security
- Surveillance & surveillance avoidance
  Trading privacy for safety? And trying to keep one's privacy
- Safe computing and networking
  Can following simple rules make you safer?

8 Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

All drawings and photos by Ben Gaucherin unless noted

Slide#   credit
2   Harvard Extension School shield
3   The IT crowd - channel4.com
4   Le penseur www.musee-rodin.fr
5   https://ia802505.us.archive.org/zipview.php?zip=/33/items/olcovers6/olcovers6-Lzip&file=61922-L.jpg
6   http://www.onelifesuccess.net/wp-content/uploads/2014/04/bernerslee-404_682192.jpg
6   https://www.flickr.com/photos/metropolismusic/2667617635
7   http://countermeasures.trendmicro.eu/royal-australian-air-force-website-defaced/
7   http://wdl.tmimgcdn.com/img_articles/22270/08.jpg
7   http://www.thevintagenews.com/wp-content/uploads/2015/05/credit.jpg
8   http://security.harvard.edu
8   "NSA Great Seal bug" by NSA - http://www.nsagov/gallery/photo/photo00023.jpg (from [1]). Licensed under Public Domain via Wikimedia Commons - https://commons.wikimedia.org/wiki/File:NSA_Great_Seal_bug.jpg#/media/File:NSA_Great_Seal_bug.jpg
8   PVIDSS logo

9 Copyright © Scott Bradner & Ben Gaucherin 2016

Introduction
E45a review

CSCI E 45b: The Cyber World – part B

1   Copyright © Scott Bradner & Ben Gaucherin 2016

What you should remember from the first semester, even if you weren't there

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

2   Copyright © Scott Bradner & Ben Gaucherin 2016

E45a Review: Digital tech & computing

Digital Technology and Computing Devices

- In cyberspace everything is bits
- What the bits mean depends on how you use them
  Bits = Data = Code
- From transistor, to wired logic, to programmable computers

3   Copyright © Scott Bradner & Ben Gaucherin 2016

E45a Review: Digital tech & computing

Mother-board of a Compaq Presario 4528

- "Power" of computers doubles every 18-24 months
  Interpretation of Moore's Law
- Generic computing devices have a consistent set of parts/components
  Firmware/Boot software, CPU, interrupts, memory, Input/Output
- Key concepts
  Interoperability, Virtualization, and Redundant Array of things

4 Copyright © Scott Bradner & Ben Gaucherin 2016

E45a Review: Internet history & concepts

Internet History and Concepts

- It all started with the telephone network but the telephone companies were not involved in Internet service until recently
- Packet networking was developed in the 1960s to create a reliable communications infrastructure
- The ARPANET was deployed starting in the last 1960s to share big computers
- The Internet started with the switch to the Internet Protocol in 1983

5 Copyright © Scott Bradner & Ben Gaucherin 2016

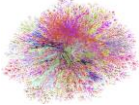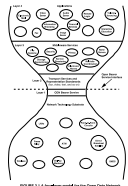## E45a Review: Internet history & concepts

- The Internet architecture is end-to-end (e2e) with a "stupid network"
  Intelligence is in the end nodes
- The Internet Protocol is a "common bearer service" that supports applications over different types of networks
  Hides network from applications and vice versa
- The Internet does not have any defined architecture

6 Copyright © Scott Bradner & Ben Gaucherin 2016

E45a Review: Internet protocols

Internet Protocols

- Internet Protocol
  - "old" Internet protocol is IPv4 – 32-bit addresses
  - "new" Internet protocol is IPv6 – 128-bit addresses
    - Many small changes between IPv4 & IPv6
- IP is very simple – its only job is to deliver packets as best as it can
  - Uses destination IP address to forward packets
- Packets can be fragmented if they are too big for the network
  - Only by the source in IPv6

7   Copyright © Scott Bradner & Ben Gaucherin 2016

E45a Review: Internet protocols

- Protocols ride on top of IP and are "end to end" (e2e)
  - Transmission Control Protocol (TCP)
    - Provides a reliable data stream with flow & congestion control
  - User Datagram Protocol (UDP)
    - Non-guaranteed packet transfers
  - Internet Control Message Protocol (ICMP)
    - Control & error messages
- For e2e protocols, only the end points are involved
  - The network is not involved

Ethernet Frame	IP Header	TCP or UDP Header	Application Header	Content Payload

8   Copyright © Scott Bradner & Ben Gaucherin 2016

E45a Review: Simple software

Software - Simple Software

- Operating systems are the runtime environment for applications and include:
  - Services, user interface, hardware drivers, utilities
- Creating an executable with compiled languages
  - Human readable programming language source code compiled to computer readable object code and linked into an executable
- Interpreted languages (e.g. BASIC)
  - A script interpreter processes the script

9   Copyright © Scott Bradner & Ben Gaucherin 2016

E45a Review: Simple software
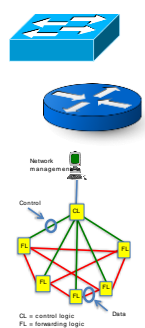
- And scripting extends to the Web
  Server side, client/browser side
- There's more to software development than just knowing a programming language – the craft
  Analytical thinking, software development lifecycle – Waterfall/Agile, versioning, coding standards, source code control, Quality Assurance/Testing, build/release

10   Copyright © Scott Bradner & Ben Gaucherin 2016

E45a Review: Simple software

- Running software uses consistent structures no matter what the runtime environment is
  Process, stack, heap, threads
- Software can be abused
  Reversing, patching with malicious bits, buffer overflow

11   Copyright © Scott Bradner & Ben Gaucherin 2016

E45a Review: Network technology

Network Technology

- Layer-based conceptual model
  Hardware at bottom, application at top
- Historic telephone system – country-based architecture
  Providing guaranteed but limited services (i.e. voice)
- Internet (generally) not country-based
  Provides many services but no guaranteed quality

12   Copyright © Scott Bradner & Ben Gaucherin 2016

E45a Review: Network technology

- Enterprise networks mixture of layer 2 and layer 3
  Layer 2 – switched Ethernet & WiFi in "subnets"
  Layer 3 – routers interconnect subnets and run Internet Protocol
- Internet service provider (ISP) architecture similar to enterprise IP networks
  Customers connected to local "points of presence" (PoPs) – parts of ISPs connected with routers
- Software defined networks (SDN) used in cloud services
  Architecture defined by software rather than wires

CL = control logic
FL = forwarding logic

13   Copyright © Scott Bradner & Ben Gaucherin 2016
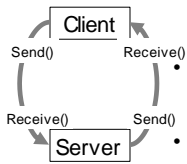
E45a Review: Distributed systems

Software – Distributed Systems

- Distributed systems are the norm in a networked world
  Complex website, large enterprise system, distributed computation, the Internet
- Basic model - Client/Server
  But every system can be both a client and a server
- Key characteristics of distributed software
  Physical separation, scalability, administrative autonomy, heterogeneity

14   Copyright © Scott Bradner & Ben Gaucherin 2016
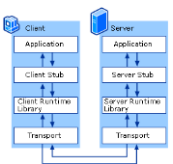
E45a Review: Distributed systems

- Distributed systems architectures have evolved greatly over the past few decades
  Mainframe, client/server 2 & 3 tier, web architectures, Service Oriented Architectures/Web Services
- Basic mechanics of software talking over a network
  Remote Procedure Call (RPC), Interface Definition Language (IDL), XML/JSON
- Servers can be stateful or stateless
  State can be stored in a variety of places (e.g., cookies)

15   Copyright © Scott Bradner & Ben Gaucherin 2016
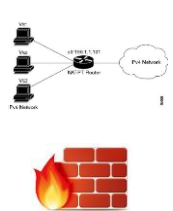
E45a Review: Middleware

Internet and Enterprise Middleware

- Network address translators (NATs)
  Join one network to another – translate IP addresses in packets that traverse NAT
  - Different inside and outside network address spaces
  Can break some protocols
- Firewalls
  Join one network to another – selectively block some traffic between networks

16   Copyright © Scott Bradner & Ben Gaucherin 2016

E45a Review: Middleware

- Proxy servers
  Intermediary between clients and servers
  - Can cache information to improve performance
  - Can hide client from server & bypass filters
- Transparent caches
  Cache information to improve performance
- Load balancers
  Intercept and distribute client requests among servers
- Content switches
  Intercept and distribute client requests among servers based on type of request

17   Copyright © Scott Bradner & Ben Gaucherin 2016
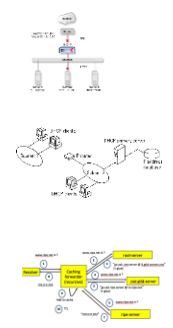
E45a Review: Middleware

- TLS/SSL accelerators
  Offload secure communications processing
- Dynamic host configuration protocol (DHCP) servers
  Supply network information to network nodes during boot process
- Domain name system (DNS) servers
  Distributed name resolution service that converts DNS names into IP addresses

18   Copyright © Scott Bradner & Ben Gaucherin 2016

E45a Review: Middleware

UPnP

- Service discovery servers
  - Enable hosts to find services such as printers
- Authentication services
  - Offloads user authentication function
  - Some can support "single sign on"
- Authorization services
  - Offloads user authorization function
    - Decides who can do what
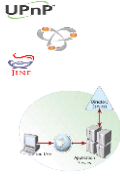
Group A=
(
{people determined by attributes}
- {people to be excluded}
+ {people to be included}
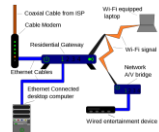)

19   Copyright © Scott Bradner & Ben Gaucherin 2016

E45a Review: Building the infrastructure

Designing and Building the Infrastructure

- The tussles
  - #1 - Optimizing resource allocation to demand/needs
  - #2 - Reconciling resiliency, security, and complexity
- Residential infrastructure
  - Single ISP, single dynamic IP address, not setup to deliver network services, not much redundancy built-in
- Enterprise infrastructure
  - Large number of IP addresses, designed for resiliency, can deliver network services, one or more ISPs
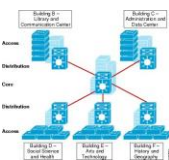
20   Copyright © Scott Bradner & Ben Gaucherin 2016

E45a Review: Building the infrastructure

- Enterprise - From the end-point to the ISP
  - Core > Distribution > Access
  - Network jack, WiFi, switches, data center, routers
- Generic Internet Service Provider architecture
  - Regional/metropolitan hubs, POPs/COs, Head-ends, local aggregation points, last mile connectivity

21   Copyright © Scott Bradner & Ben Gaucherin 2016

E45a Review: The cloud

NIST SP 800-145

The Cloud

- Three main services:

  Infrastructure as a Service (IaaS)
  > You create and manage servers and network in the cloud

  Platform as a Service (PaaS)
  > Servers with full technology stacks ready to receive your software

  Software as a Service (SaaS)
  > Using software operated and managed by others

22   Copyright © Scott Bradner & Ben Gaucherin 2016

E45a Review: The cloud

- Essential characteristics

  Broad network access

  Resource pooling

  Rapid elasticity

  Measured service

  On-demand self-service

23   Copyright © Scott Bradner & Ben Gaucherin 2016

E45a Review: The cloud

ITU-T X.1600

- Some challenges

  Trusting the provider
  > Governance of technical decisions
  > Privacy
  > Security
  > Business

  Availability

  Lock-in

24   Copyright © Scott Bradner & Ben Gaucherin 2016
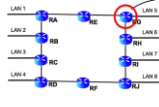
E45a Review: Routing

Enterprise and ISP Routing

- "Routing" is forwarding packets towards a destination
  - Using a destination address that is in the packet
- Routers exchange reachability information using a routing protocol
  - Use info. to build a "routing table"
  - Sends packet to next hop on "best path" to destination
- Two categories of routing protocols
  - Interior gateway protocols (IGPs)
  - Exterior gateway protocols (EGPs)
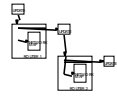
25   Copyright © Scott Bradner & Ben Gaucherin 2016

E45a Review: Routing

- Interior gateway protocols
  - Assume a unified trust domain
  - Routing information protocol (RIP)
    - Simple "distance vector" protocol
    - Builds table of "lowest cost" next hops for possible destinations from updates that include reachability metric
  - Open shortest path first (OSPF)
    - Link state protocol
    - Builds network topology map from updates that include link information
    - Builds table of "lowest cost" next hops for possible destinations from information in network topology map

26   Copyright © Scott Bradner & Ben Gaucherin 2016

E45a Review: Routing

- Exterior gateway protocol
  - Does not assume trust
  - Border gateway protocol (BGP4)
    - Builds table of paths to possible destinations from updates that include paths to possible destinations
    - Includes comprehensive tools to filter updates received and sent to control reachability

27   Copyright © Scott Bradner & Ben Gaucherin 2016

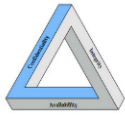## E45a Review: Security fundamentals

Security Fundamentals

- **"Security" means ensuring:**
  Confidentiality, Integrity & Availability (C.I.A.)
- **Security issues**
  Failure to take care of the basics, people, buggy software, flawed computer/network setup/configuration, aiming for perfection, secrecy is not security (Kerckhoff principle)
- **Understanding risk**
  Humans not good at assessing risk
  - An approach: Identify risk, assess likelihood & impact, prioritize, mitigate

28   Copyright © Scott Bradner & Ben Gaucherin 2016

E45a Review: Security fundamentals

- **Threat is a component of risk**
  Need to identify the asset, threats to that asset, and probability of the threat being realized
- **Attack trees**
  A more formal approach to analyzing threats
- **Mitigations**
  Principles of secure software development, securing the physical environment, designing secure data networks, the risks of portable media, the risks of residual data on disk drives, enterprise security policies
- **Crustacean security**

29   Copyright © Scott Bradner & Ben Gaucherin 2016

E45a Review: Encryption

Encryption

- **Encryption – basic confidentiality tool**
  Mathematically obscuring data in a reversible way
  Symmetric encryption systems
  - One time pad, Enigma, DES, 3DES, AES
  Asymmetric encryption systems
  - Public key encryption – Public/Private keys
- **Hashes – basic integrity tool**
  Creating a unique fingerprint of a chunk of data
  Basic hash, keyed hash

30   Copyright © Scott Bradner & Ben Gaucherin 2016

E45a Review: Encryption

- **Digital Signatures**
  - Hash of message encrypted with private key, verified with public key
    - Provides integrity, authentication of origin/non-repudiation
- **Digital Certificates**
  - Public key with one or more digital signatures
  - To securely convey public keys
- **Certificate Authorities**
  - A source of digital certificates
  - Lots of CAs, with varying trustworthiness

public key

signature

31

Copyright © Scott Bradner & Ben Gaucherin 2016

E45a Review: Managing the infrastructure

Managing the Infrastructure

- **What are you managing?**
  - Managing evolution, managing operations
  - Managing the technology, the business, the experience of the user of the services
- **Management frameworks**
  - Many of them, but you should still be thinking for yourself
- **ITIL – a good framework for services**
  - Service Strategy, Service Design, Service Transition, Service Operation, Continual Service Improvement

ITIL®

32

Copyright © Scott Bradner & Ben Gaucherin 2016

E45a Review: Managing the infrastructure

- **Management tools**
  - Telephone world – large, complex holistic set of tools
  - Internet world – simple, point solutions focused on reliable packet delivery
- **SNMP & NETCONF**
  - IETF standards for managing IP networks and device configurations
- **Business Continuity (BC) & Disaster Recovery (DR)**
  - Adjusting to suddenly changing conditions
  - DR is asynchronous resiliency
  - Business Impact Analysis (BIA), Mean Time To Fail (MTTF), Mean Time To Recovery (MTTR)

33

Copyright © Scott Bradner & Ben Gaucherin 2016

E45a Review: Security tools

Security Tools

- Blocking tools – selectively block traffic
  - Access Control Lists (ACLs), firewalls, Application Level Gateways (ALGs), virus checkers, spam filters, intrusion prevention, Network Access Controls (NACs)
- Detecting tools – monitor and/or flag "abnormalities"
  - Packet sniffers, intrusion detection, file integrity checkers,
- Probing tools – look for "soft spots"/vulnerabilities
  - Vulnerability detection, compliance monitoring

34 Copyright © Scott Bradner & Ben Gaucherin 2016

E45a Review: Security tools

- With every tool, be mindful of dual use
- Offensive security tools – active security investigation and/or disruption
  - Packet generators/manglers/fuzzers, hijacking tools, brute force tools, fingerprinting tools

35 Copyright © Scott Bradner & Ben Gaucherin 2016

E45a Review: Internet regulations

Internet Regulation

- Telephone world is very well regulated
  - Regulations control technology, services, prices, & use
  - International regulations from International Telecommunications Union (ITU)
  - Plus national regulations - e.g., from Federal Communications Commission (in U.S.)
- Internet is essentially unregulated
  - Major current conflict over the "need" to regulate the Internet

36 Copyright © Scott Bradner & Ben Gaucherin 2016

E45a Review: Internet standards

Standards development

- Telephone standards developed by traditional standards organizations (e.g., ITU)

  Members-only process

  Consensus-based approval by government representatives

37   Copyright © Scott Bradner & Ben Gaucherin 2016

E45a Review: Internet standards

- Internet-related technology standards are developed by the IETF

  Open process, you-too can participate

  "rough consensus" approval by technical community

38   Copyright © Scott Bradner & Ben Gaucherin 2016

E45a Review: Wrapup

- This has been a review for some of you, for others it may be a preview
- In any case, this is useful information for you to have (even if it won't be on the exams)
- And it gives you additional information and context on what this course is about

39   Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

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

Slide#   credit
4   "LED traffic light" by Bidgee - Own work. Licensed under CC BY 3.0 via Wikimedia Commons -
https://commons.wikimedia.org/wiki/File:LED_traffic_light.jpg#/media/File:LED_traffic_light.jpg
5   tech-kid.com
            Drawing from Baran 1962 paper
            Diagram: RFC 791
6   Hourglass diagram: Realizing the Information Future
            Internet map - Bill Cheswick
9   "Green Dragon Book (front)" by Source (WP:NFCC#4). Licensed under Fair use via Wikipedia - https://en.wikipedia.org/wiki/
10   http://popdigital.ca/wp-content/uploads/2013/03/triangles.png
15   https://i-technet.sec.s-msft.com/dynimg/IC196578.gif
16   nat - http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-15-mt-book/ip6-natpt.html
            firewall - Source: http://computerservernetwork.com

40   Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

Slide#   credit
17   proxy - https://forrester-infosystems.wikispaces.com/Proxy+servers
            load balancer - http://community.citrix.com/display/cdn/Load+Balancing
            content switch - http://blogs.citrix.com/2014/10/24/got-database-netscaler-datastream-technology-addresses-explosive-growth/
18   ssh offload - https://support.f5.com/kb/en-us/archived_products/big-ip/manuals/product/bigip4_5admin/bigip_sslgate.html
            dhcp -
https://www.microsoft.com/resources/documentation/windowsnt/4/server/reskit/en-us/net/sur_dhcp.mspx?mfr=true
            dns – www.ripe.net (do not know the full url)
19   upnp - http://dev.bukkit.org/bukkit-plugins/upnp/images/1-upnp/
            bonjour - http://news.oreilly.com/2008/06/
            jini - http://www.coroflot.com/ariamiller/logo
            auth - http://pamungkaswave.blogspot.com /
20   "Homenet" by Lucid - Own work. Licensed under CC BY-SA 3.0 via Commons -
https://commons.wikimedia.org/wiki/File:Homenet.svg#/media/File:Homenet.svg
21   http://www.cisco.com/c/dam/en/us/td/i/200001-300000/220001-230000/227001-228000/227530.eps/
22   NIST SP800-145 visual http://www.ibm.com/developerworks/cloud/library/cl-extenddevtocloudbigdata/nist-cloud.gif

41   Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

Slide#   credit
24   ospf https://capaocho8.com/configuracion-de-ospf-con-ipv4-e-ipv6-para-ios-cisco-xr-parte-1/
26   cia - http://www.digitalthreat.net/2011/12/anti-virus-wont-keep-your-data-safe/
            hand http://mathsloverhubpages.com/hub/How-to-calculate-probabilty
27   https://www.pinterest.com/secawareness/security-fail/
28   https://en.wikipedia.org/wiki/File:Enigma-machine-bob-lord.jpg
30   ITIL logo http://community.gbtribune.com/blogs/detail/790/
31   http://www.kitsch-slapped.com/wp-content/uploads/2011/01/1950-snake-oil-is-wonderful-stuff.jpg
32   leak stop - http://www.supercool.ac/products/leak-stop/
            SNORT https://en.wikipedia.org/wiki/Snort_%28software%29
33   John - http://www.cybercrimetech.com/2014/07/how-to-cracking-zip-and-rar-protected.html
            Hydra - https://h4xors.wordpress.com/2012/06/09/hacking-email-accounts-with-hydra/
34   itu – www.itu.int
            fcc - https://transition.fcc.gov/files/logos/fcc-logo_black.png
            bee - http://www.vermontinsects.org/bees.html
35   itu – www.itu.int
            http://www.3gpp.org/about-3gpp/18-3gpp-logo-use
36   https://www.ietf.org/logo/
42   Copyright © Scott Bradner & Ben Gaucherin 2016