


Security fundamentals
Introduction

CSCI E 45a: The Cyber World – part A

1 Copyright © Scott Bradner & Ben Gaucherin 2015

Learning goals



- Understand what the term “information security” refers to
- Understand the role of secrecy in information security
- Understand the basics of risk and threats and how to gage them
- Understand some of the threat mitigation approaches

2 Copyright © Scott Bradner & Ben Gaucherin 2015

Introduction: this module

- This module deals with a mixture of technology, policy and operations practice

3 Copyright © Scott Bradner & Ben Gaucherin 2015

Topics (all required)



- **What is information security?**
Overview of the aspects of information security



- **Understanding risk**
How to understand risk, even though people are quite bad at doing so



- **Attack trees**
Bruce Schneier's method of risk evaluation

4

Copyright © Scott Bradner & Ben Gaucherin 2015

Topics (all required)



- **Threat mitigation I**
Good software development & securing the physical environment



- **Threat mitigation II**
Designing secure networks



- **Threat mitigation III**
Portable media & residual data on disk drives



- **Threat mitigation IV**
Enterprise security policies

5

Copyright © Scott Bradner & Ben Gaucherin 2015

Image credits

All drawings and photos by Scott Bradner unless noted

Slide# credit

4 cia - <http://www.digitalthreat.net/2011/12/anti-virus-wont-keep-your-data-safe/>

hand <http://mathslover.hubpages.com/hub/How-to-calculate-probability>

Schneier - <https://www.schneier.com/>

5 chain -

<https://www.pinterest.com/secawareness/security-fail/>

firewall - <http://www.firemon.com/advancing-firewall-necessary-evils-10-tuple/>

tumb drive - <http://www.amazon.com/PNY-Turbo-256GB-Flash-Drive/dp/B00JN1TOHM>

hat - <http://www.yeehawcowboy.com/Los-Altos-Hats-Joan-Style-Felt-Cowboy-Hat-4x-6x-10x-Available-Joan-brim-felt-cowboy-hat-1-13.htm>

6


Copyright © Scott Bradner & Ben Gaucherin 2015

Security fundamentals
What is Information Security?

CSCI E 45a: The Cyber World – part A

1 Copyright © Scott Bradner & Ben Gaucherin 2015


Information Security




- What is information security?
“The protection of automated information from unauthorized access (accidental or intentional), modification, destruction, or disclosure.”
- California State Administrative Manual

2 Copyright © Scott Bradner & Ben Gaucherin 2015

The “other” C.I.A.



Dara Epp

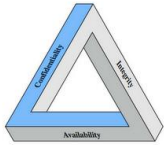


Dorn B. Parker

- CIA
 - Confidentiality
 - Integrity
 - Availability
- Parkerian hexad
 - CIA + Possession or Control
 - Authenticity
 - Utility

3 Copyright © Scott Bradner & Ben Gaucherin 2015

C.I.A. and security problems



- Security problems can be described in how they affect C.I.A.
 - DoS/DDoS – Availability
 - Spyware – Confidentiality
 - Key loggers – Confidentiality
 - Phishing – Confidentiality, Integrity
 - Etc.

4

Copyright © Scott Bradner & Ben Gaucherin 2015

A brief history of InfoSec



1834: disposal of tally sticks
1945: "first" computer "bug"
(*"found a bug that was a real bug"*)



1964: "phone freaks"
1972: first mention of virus:
David Gerrold: *"When Harlie Was One"*



1978: first spam
DEC employee Carl Gartley



1979: first worm implemented:
Xerox PARC

5

Copyright © Scott Bradner & Ben Gaucherin 2015

A brief history of InfoSec, contd.



1983: break-ins on US government nets (the '414s')



Cliff Stoll

1985: Robert Morris describes SYN attack
1986: "The Brain" PC virus in the wild (Pakistani programmers)
1986: *"The Cuckoo's Egg"* (Cliff Stoll) break in

6

Copyright © Scott Bradner & Ben Gaucherin 2015

A brief history of InfoSec, contd.



7

- 1987: XMAS virus (EARN and IBM corporate network)
- 1988: the Morris worm
- 1989: CERT formed (in response to Morris worm)
- 1980s: Nigerian ("419") Scam initially via fax, moved to email in '90s
- 1994: first high-profile spam Phoenix lawyers Canter and Siegel
- 1996: SYN attacks start
- 1999: "Melissa" virus \$80M damage

Copyright © Scott Bradner & Ben Gaucher in 2015

A brief history of InfoSec, contd.



8

- 2000: SYN attack on Yahoo!
- 2001: Code Red (\$2B damage)
- 2002: DoS attack on DNS root servers
- 2003: Slammer worm (first Warhol worm)
- 2003: first "good" Phishing
- 2004: "MyDoom" e-mail worm (social engineering)
- 2004-5: \$7.8B cost to repair or replace infected computers

Copyright © Scott Bradner & Ben Gaucher in 2015

A brief history of InfoSec, contd.



9

- 2006: Wikileaks founded
- 2010: Stuxnet - targeted Iran
- 2013: Edward Snowden - revealed NSA operations
- 2014: Sony hacked by North Korea
- 2015: US personnel office hacked by Chinese
- 2019: Facebook 500M accounts
- 2020: SolarWinds
- 2021: Colonial Pipeline ransomware

Copyright © Scott Bradner & Ben Gaucher in 2023



Failure to take care of the basics



- Underlying security problems have not changed that much over time

“According to virus incident reports as well as network users, weaknesses at host sites included (1) inadequate attention to security, such as poor password management, and (2) systems managers who are technically weak”

Virus Highlights Need for Improved Internet Management
US GAO June 1989 (study in response to the Morris worm)

10

Copyright © Scott Bradner & Ben Gaucherin 2015

Other Security Issues, contd.



- People
confused people, lazy people, evil people
- Buggy software
- Flawed computer setup and configuration
- Flawed network configuration

11

Copyright © Scott Bradner & Ben Gaucherin 2015

Other Security Issues, contd.



I E T F

btns WG

- Perfection level
Security “experts” who insist: perfection or worthless
But real world works on “good enough security”
i.e., security to balance the threat, not to be perfect
Aim: make the cost of exploiting greater than the value realized

12

Copyright © Scott Bradner & Ben Gaucherin 2015

Other Security Issues, contd.



Auguste Kerckhoffs

- Secrecy is not security
Surprisingly, many people think that secrecy creates security
Auguste Kerckhoffs (1883)

The design of a system should not require secrecy

Bruce Schneier

every secret creates a potential failure point

- i.e., security through obscurity (by itself) is very bad security

You should assume that the bad guys find out all your secrets (other than the key itself)



Bruce Schneier

13

Copyright © Scott Bradner & Ben Gaucherin 2015

Image credits

All drawings and photos by Scott Bradner unless noted

Slide# credit

3 app -

<http://www.runasradio.com/default.aspx?showNum=245>

parker - <https://www.linkedin.com/pub/donn-b-parker/4/b28/449>

4 <http://www.digitalthreat.net/2011/12/anti-virus-wont-keep-your-data-safe/>

6 brain - <http://www.neatorama.com/2012/05/04/going-viral-the-first-pc-virus/>

stoll - <http://likesuccess.com/author/clifford-stoll>

7 xmas virus - <https://thesprawl.org/simstim/day-technopath/>

morris -

<http://www.computerhistory.org/revolution/networking/19/378/2>

159

cantor & -

<https://www.flickr.com/photos/treborschclz/3043385467>

14

Copyright © Scott Bradner & Ben Gaucherin 2015

Image credits

All drawings and photos by Scott Bradner unless noted

Slide# credit

8 warhol -

http://www.huffingtonpost.com/2013/04/19/andy-warhol-house-for-sale-upper-east-side-townhouse_n_3115150.html

9 snowden -

https://en.wikipedia.org/wiki/Edward_Snowden

interview - <http://www.imdb.com/title/tt2788710/>

11 <http://www.zwallpix.com/group-of-people.html>

13 kerckhoffs -

<https://commons.wikimedia.org/wiki/File:Kerckhoffs.jpg>

Schneier - <https://www.schneier.com/>

15

Copyright © Scott Bradner & Ben Gaucherin 2015


Security fundamentals
Understanding risk

CSCI E 45a: The Cyber World – part A

1 Copyright © Scott Bradner & Ben Gaucherin 2015

Risk

- People are poor at actually categorizing risk
Which is safer – driving or commercial flying?
Driving: 1.35 fatalities per 100 million miles in 2022
Commercial airlines: 0.0 fatalities per 100 million miles in 2022 in US
- Cost complicates things
Cost of airbags is about \$1.8M/life saved
(Maybe more if you take seatbelt non-use into account)
Dubner – *SuperFreakonomics*





Stephen J. Dubner

2 Copyright © Scott Bradner & Ben Gaucherin 2023

Risk Analysis & Mitigation

- 1st problem in security is to understand what threats you actually face
Do not ignore threats from inside the organization
Note that non-compliance with laws or regulations can be a threat by itself
- Then understand the probability that a threat will be realized and the damage if it is



3 Copyright © Scott Bradner & Ben Gaucherin 2015

Risk Analysis & Mitigation, contd.



worst-case scenario
(no product endorsement implied)

- Then **mitigate threats** that are seen as significant
Assuming service is still worth offering
(Considering threats)

4

Copyright © Scott Bradner & Ben Gaucherin 2015

Risk Analysis & Mitigation, contd.

For your convenience we no longer accept cash.



- Threat mitigation can involve many approaches
Revising procedures
Revising or switching applications
Deploying different technology
Stop providing an at-risk service
- Must **assume all exploits are known by someone**
e.g., ex-employee
'security through obscurity - by itself' is not security
e.g., Google finding student files
User of "site." was called a "malicious cyber actor"

5

Copyright © Scott Bradner & Ben Gaucherin 2015

Threat Models



- **Threat model:** way to understand and prioritize risks and evaluate mitigation possibilities
- Steps to a threat model
Identify assets
Understand system
Understand threats
Categorize threats
Rank the threats
- Develop mitigation strategies for high ranking threats

6

Copyright © Scott Bradner & Ben Gaucherin 2015

Threat Models: Identify Assets

- What is it that you are trying to protect?
e.g., Social Security numbers, camera, airplane ...
- Note: you are not trying to “protect an application”
Unless you are worried about someone stealing the software or stealing a license for the software
- In other words: “*You are not trying to protect the safe, rather you are trying to protect the thing in the safe.*”

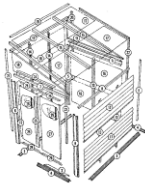


7

Copyright © Scott Bradner & Ben Gaucherin 2015

Threat Models: Understand System

- Understand the system architecture
computer system, application, organization ...
- Deconstruct the architecture to understand its parts



8

Copyright © Scott Bradner & Ben Gaucherin 2015

Threat Models: Understand System, contd.

- Understand the interfaces within the architecture
 - Entry & exit points
Between user and system & between systems
 - Trust & privilege boundaries
Where is trust assumed or privilege accepted?
 - Data flows
How does data flow in system?
e.g., does checkpoint have data needed to perform check?



9

Copyright © Scott Bradner & Ben Gaucherin 2015

Threat Models: Understand Threats

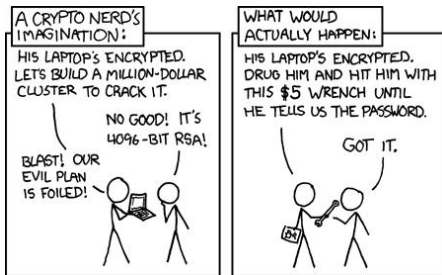
- Understand how adversary might attack system
Assume adversary knows all of the vulnerabilities
- Multiple ways to find or evaluate threats
 - History/experience
 - e.g., personal experience with similar systems
 - e.g., read reports about exploits
 - Vulnerability databases
 - e.g., virus fingerprints, Common Vulnerabilities and Exposures (CVE)
 - Attack trees



10

Copyright © Scott Bradner & Ben Gaucherin 2015

Understanding Threats- Example



Copyright © Scott Bradner & Ben Gaucherin 2015

11

Threat Models: Categorize Threats

- Understand types of threats
- e.g., using **STRIDE** (Microsoft)
 - S**poofing - assume a false identity
 - T**ampering with data - modify data
 - R**epudiation - insufficient log info to track attacker
 - I**nformation disclosure - gain access to protected info
 - D**enial of service - impact access/use by legitimate users
 - E**levation of privilege - perform actions not normally permitted



12

Copyright © Scott Bradner & Ben Gaucherin 2015

Threat Models: Rank the Threats

- Understand the relative importance of the threats
- e.g., using DREAD (Microsoft)
 - Discoverability - how hard is it for an attacker to find exploit
 - Reproducibility - how easy to turn threat into an attack
 - Exploitability - how much expertise is required
 - Affected users - how many users will be affected
 - Damage potential - cost of damage



13

Copyright © Scott Bradner & Ben Gaucherin 2015

What is the worst that could happen?



- Risks to life are special
 - Another risk calculation: "minimizing regret"
 - i.e., how would you feel if the threat came true?

14

Copyright © Scott Bradner & Ben Gaucherin 2015

Threat Models: Mitigation Strategies



- Determine what can be done to mitigate high ranking threats
 - May be best to stop service, at least for a while
- Select countermeasures from those that would mitigate the threat
 - May require a combination of countermeasures
 - Compare cost and effectiveness

15

Copyright © Scott Bradner & Ben Gaucherin 2015

Image credits

All drawings and photos by Scott Bradner unless noted

Slide#	credit
2	plane http://www.clicer.com/clipart-6890.html car http://canwallstar.com/orange-car-clip-art-vector-clip-art-online-royalty-free/car-clipart-images/clip-art-images-of-a-car-clipart-best-gtkkpn/ dubner http://stephenjdubner.com/bio.html
3	zombie http://www.clipartpanda.com/clipart_images/original-zombie-clip-art-26268153 hand http://mathsloverchubpages.com/hub/How-to-calculate-probability
4	http://www.margaretmeloni.com/Mitigateyourself.html
6	http://onlinejournalismblog.com/2014/07/16/why-every-journalist-should-have-a-threat-model-with-cats/

16

Copyright © Scott Bradner & Ben Gaucherin 2015

Image credits

All drawings and photos by Scott Bradner unless noted

Slide#	credit
7	safe - http://wallpaperswide.com/safe_deposit_box-wallpapers.html
8	http://www.searspartsdirect.com/model-part/ys475b/0067/1500040/00013415/00001.html
9	http://www.dualwarez.com/2012/11/funny-indian-signs.html http://depositphotos.com/5600657/stock-photo-binary-data-flow.html
10	http://www.coolnsmart.com/history_quotes/
11	http://xkcd.com/538/
12	http://www.blurent.com/article/23-intriguing-facts-that-make-fun-of-threat-modeling
14	https://commons.wikimedia.org/wiki/File:Paris_Tuileries_Garden_Facepalm_statue.jpg
15	
17	http://www.kcet.org/updaily/social-focus/commentary/w


15

Security fundamentals
Attack trees

CSCI E 45a: The Cyber World – part A

1 Copyright © Scott Bradner & Ben Gaucherin 2015

Attack Trees



Attack trees provide a formal, methodical way of describing the security of systems, based on varying attacks.

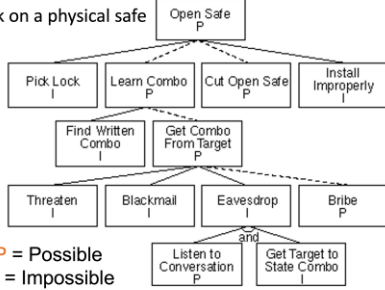
Bruce Schneier

- Attacks against a system represented in a tree structure
 - With attack goal as the root node
 - An important question to ask: what is the goal?
 - With different ways of achieving that goal as leaf nodes

2 Copyright © Scott Bradner & Ben Gaucherin 2015

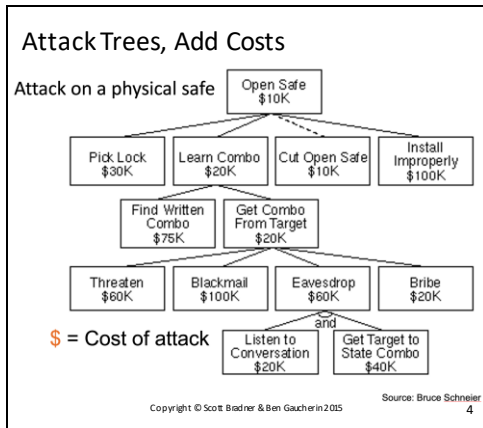
Attack Trees, Sample

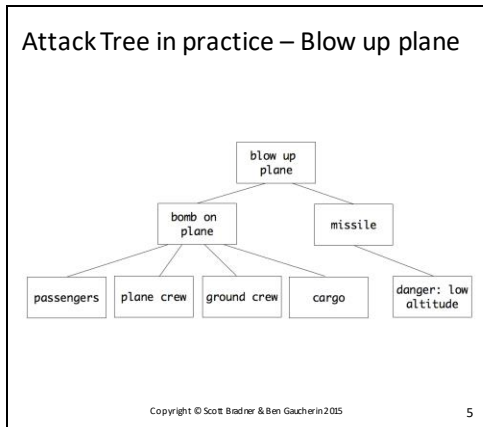
Attack on a physical safe

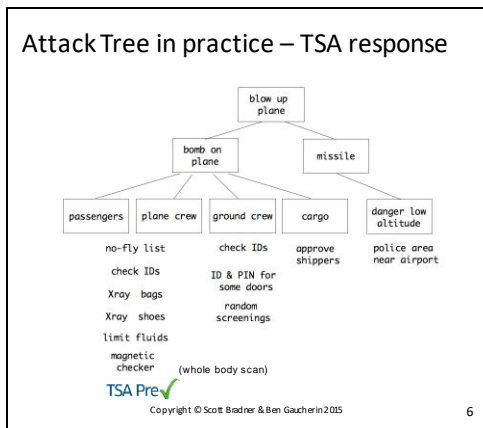


P = Possible
I = Impossible

Source: Bruce Schneier
Copyright © Scott Bradner & Ben Gaucherin 2015 3







Attack Tree in practice – TSA response



- Liquid explosives
British reported a plot to use liquid explosives on a plane
Explosives experts say it's very hard to create explosive from raw materials in plane-like environments - so real threat level is hard to evaluate
1st pass: passengers – no liquids into plane
Even liquids delivered planeside by duty free shops - what underlying threats is this effective against?

7

Copyright © Scott Bradner & Ben Gaucherin 2015

Attack Tree in practice – TSA response



Copyright © Scott Bradner & Ben Gaucherin 2015

8

Another attack tree example

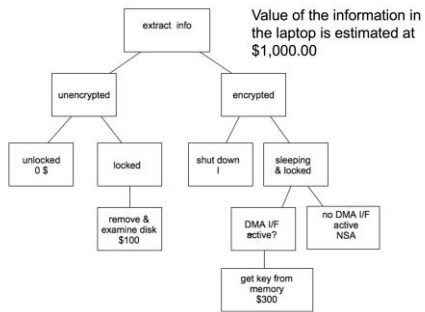


- Assume you have valuable information on your laptop & it gets stolen or lost
- Assume it was a targeted theft
You were targeted because the thief knew you had the valuable information
- **Question:** is laptop encryption worth the effort and cost?

9

Copyright © Scott Bradner & Ben Gaucherin 2015

Another attack tree example, contd.



Copyright © Scott Bradner & Ben Gaucherin 2015

10

Image credits

- All drawings and photos by Scott Bradner unless noted
- | Slide# | credit |
|--------|---|
| 2 | Schneier https://www.schneier.com/ |
| 8 | http://vitalsignsblog.blogspot.com/2012/08/former-ta-boss-airline-security-is-bust.html |
| 7 | http://www.examiner.com/article/tsa-restrictions-for-liquid-carry-ons |
| 9 | http://www.clker.com/clipart-14767.html |

11


Copyright © Scott Bradner & Ben Gaucherin 2015

Security fundamentals
Threat mitigation I

CSCI E 45a: The Cyber World – part A

1 Copyright © Scott Bradner & Ben Gaucherin 2015


Some threat mitigation areas




- Principles of secure software development
It helps if the software itself is secure
- Securing the physical environment
Making sure the bad guy can not walk in the door

2 Copyright © Scott Bradner & Ben Gaucherin 2015

Secure Software Development



Jerry Saltzer



Michael Schroeder

- Principles of Secure Software Development:
Saltzer and Schroeder (1974)
 1. Economy of mechanism:
Keep the design as simple and small as possible.
 2. Fail-safe defaults:
Base access decisions on permission rather than exclusion.
 3. Complete mediation:
Every access to every object must be checked for authority.
 4. Open design:
The design should not be secret.

3 Copyright © Scott Bradner & Ben Gaucherin 2015

Secure Software Development, contd.

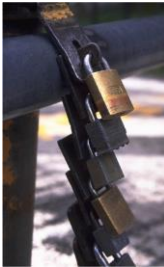


- 5. Separation of privilege:
... a protection mechanism that requires two keys... it is more robust and flexible than one that allows ... only a single key.
- 6. Least privilege:
Every program and every user of the system should operate using the least set of privileges necessary to complete the job.
- 7. Least common mechanism:
Minimize the amount of mechanism common to more than one user
- 8. Psychological acceptability:
...the human interface [should] be designed for ease of use, so that users routinely and automatically apply the protection mechanisms

4

Copyright © Scott Bradner & Ben Gaucherin 2015

Securing the Physical Environment



- Parts of physical security
 - Intrusion prevention
 - Intrusion detection
 - Environmental protection
 - Disaster recovery
- Computer & Communications Security - James Arlin Cooper*

5

Copyright © Scott Bradner & Ben Gaucherin 2015



And Watch for Weak Links



Copyright © Scott Bradner & Ben Gaucherin 2015

6

Intrusion Prevention






- Physical barriers
 - Solid walls (no windows, also real walls, not sheetrock)
 - Fences
 - Network cables in conduits
- Mantraps
- Locks
 - Locked manholes
 - Locked doors
 - Locked equipment
 - Locked barriers

Barrier Angelucci

7 Copyright © Scott Bradner & Ben Gaucherin 2015


Problems With Mechanical Locks



- Some locks poorly designed
 - e.g., open Kryptonite lock with Bic pen
 - e.g., some in-line combination locks
- Easy to make a pass key for some locks
 - See Matt Blaze's paper
- Easy to jam: DoS attack
 - e.g., glue in key slot
- Hard to keep an access log
 - i.e., who entered
- Most locks can be picked

8 Copyright © Scott Bradner & Ben Gaucherin 2015

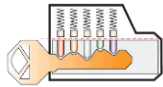
Problems With Mechanical Locks, contd.



- Keys can be copied
 - This is a picture of key to Diebold voting machine from the Diebold web site (since removed from the site)
 - Keys made from picture could open every Diebold voting machine
 - i.e., the same key worked in every machine

9 Copyright © Scott Bradner & Ben Gaucherin 2015

Picking Tumbler Locks



- A tumbler lock contains a row of split tumblers
Key lines up splits with cylinder edge
- Lock picking depends on slop in the mechanism
Put torque on cylinder
manipulate tumblers while applying pressure with lock pick until they hang up



10

Copyright © Scott Bradner & Ben Gaucherin 2015

Lock Bumping



- Can open common tumbler locks in a few seconds
Get any key that fits the lock
File cuts down to deepest depth
Put key in lock & apply torque
Hit lock
Top tumblers “bounce” & get hung above cylinder split



11

Copyright © Scott Bradner & Ben Gaucherin 2015

Issues with Barriers

- Proper placement is important



Copyright © Scott Bradner & Ben Gaucherin 2015

12

Issues with Barriers, contd.



Copyright © Scott Bradner & Ben Gaucherin 2015

13

Intrusion Prevention, contd.



- Electronic locks
e.g., wireless RFID locks, card swipe access
Can create access log
Policy/privacy issues with such logs



- Guards
- Psychological deterrence
Warning signs
Illumination
Asset tagging
Fishbowl effect



14

Copyright © Scott Bradner & Ben Gaucherin 2015

Intrusion Detection



- Surveillance
Cameras
Guards
Asset tags



- Sensors
Motion
Heat
Capacitance
Interruption
e.g., light beam, magnetic



15

Copyright © Scott Bradner & Ben Gaucherin 2015

Image credits

All drawings and photos by Scott Bradner unless noted

Slide#	credit
2	https://commons.wikimedia.org/wiki/File:KilkennyCastleDoor.jpg
3	saltzer - http://web.mit.edu/saltzer/ Schroeder http://msrsvc.org/
4	http://cs210.hubner.org/wiki/index.php?title=File:Least_privilege.png
5	http://www.bbb.org/blog/2012/06/is-my-social-security-number-safe/
6	https://www.pinterest.com/secawareness/security-fail/
7	http://www.autospec.co.za/browse.php?id=1660957461
8	top http://www.engadget.com/2004/09/14/kryptonite-evolution-2000-u-lock-hacked-by-a-bic-pen/ bottom: http://www.harborfreight.com/combo-cable-bike-lock-66689.html
16	

Copyright © Scott Bradner & Ben Gaucherin 2015

Image credits

All drawings and photos by Scott Bradner unless noted

Slide#	credit
9	http://blackboxvoting.com/s9/index.php?/categories/8-Diebold-Follies
10	http://www.blackscoutsurvival.com/p/lockpicking-101.html
11	http://www.lockwiki.com/index.php/Bumping
12	http://www.anyclip.com/movies/blazing-saddles/tollbooth/
13	http://www.wastedmoments.com/archives/33
14	http://www.intercomrus.com/digital_coded_keypad_finder_tool.htm https://icons8.com/web-app/2354/ffd-tag https://icons8.com/web-app/2354/ffd-tag
17	http://tampabay.jobing.com/blog_post.asp?post=6162 http://www.cdw.com/shop/products/WASP-KIMDURA-ASSET-TAG-2101-3100/1052505.aspx

Copyright © Scott Bradner & Ben Gaucherin 2015

Image credits

All drawings and photos by Scott Bradner unless noted

Slide#	credit
15	http://www.bbc.co.uk/jersey/content/ecards/geese_ecard.shtml
	http://www.2mcctv.com/product_info-BOSCHVEZ221.html
	http://www.safetied.org/browseproducts/Enforcer-Indoor-Outdoor-Wall-Mounted-Photoelectric-Beam-Sensor-with-35-Foot-Range.HTML


Copyright © Scott Bradner & Ben Gaucherin 2015

Security fundamentals
Threat mitigation II: designing secure networks

CSCI E 45a: The Cyber World – part A

1 Copyright © Scott Bradner & Ben Gaucherin 2015

Designing Secure Data Networks: don'ts




- Don't assume all users are trustworthy
- Don't assume users will act rationally, the way you expect them to, or that they can be trained
- Don't assume you will know exploits before the bad guys
- Don't assume systems themselves are secure
- Don't assume a peripheral firewall will cure all ills

News story: 10% of Facebook users are not human

2 Copyright © Scott Bradner & Ben Gaucherin 2015

Designing Secure Data Networks: do's



- Do assume all laptops will get stolen
- Do assume all communications will be overheard
- Do assume all email will be posted to the Net

Not just the NSA

3 Copyright © Scott Bradner & Ben Gaucherin 2015

Strategies for Secure Networks



- **Compartmentalize network**
Segment network with routers and firewalls
- **Secure individual LANs**
Router Access Control Lists (ACLs), firewalls
- **Secure user computers**
Few accounts, host based firewalls, virus protection, etc.
- **Secure servers**
Few services, few accounts, host based firewalls, virus protection, data not directly externally accessible

4

Copyright © Scott Bradner & Ben Gaucherin 2015

Strategies for Secure Networks, contd.



- **Secure communications – data in transit**
Encrypt data in transit
- **Secure data at rest**
- **Good access control**
- **Control access to network**
- **Know what you (or others) did**

5

Copyright © Scott Bradner & Ben Gaucherin 2015

Crustacean Security



- **Installing firewalls can install complacency**
Users assume they are protected
- **But open to everyone inside the wall**
Including compromised laptops
- **Only real security is end-to-end**
- **But firewalls do help**
If properly placed and are required by some regulations

6

Copyright © Scott Bradner & Ben Gaucherin 2015

Defense in Depth



- Should not just have one-layer of security
- Firewalls & filters at all levels from external Internet connection to LAN segment
e.g., do not assume everyone at a location is trustworthy
- Firewalls/filters should be put as close to the systems being protected as possible
Default configuration should only enable approved applications, input & output

7

Copyright © Scott Bradner & Ben Gaucherin 2015

Compartmentalize

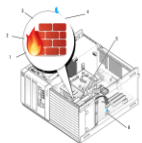


- Segment network - i.e., compartmentalize
Use switches not hubs
Segment traffic so only traffic to a particular host gets to that host
Except unknown hosts and broadcast traffic
Not perfect
Can spoof ARP, flood CAM
Local VLANs can help
But minimize wide area VLANs
Use subnets (i.e., routers)

8

Copyright © Scott Bradner & Ben Gaucherin 2015

Secure The User Computers



- Few accounts
Only have accounts for people who need access
- Host firewalls
Run host-based firewalls which block all traffic except for needed applications
Ideally: inbound & outbound
- Virus scanners
Run virus/worm/spyware scanners
Update signature lists at least daily (hourly?)

9

Copyright © Scott Bradner & Ben Gaucherin 2015

Secure The User Computers, contd.

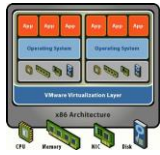


- Patch machines, quickly
Attacks can come within hours of a patch release
- Use disk encryption
Critical for laptops, useful for desktops

10

Copyright © Scott Bradner & Ben Gaucherin 2015

Secure Servers

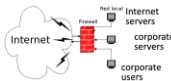


- Protect servers like hosts
- Only run the services that are actually needed
- Minimize multi-use servers
A successful attack on one service compromises others
Can use virtualization to get multiple logical servers on same physical box
- Should have firewalls between servers and ALL users (including managers)

11

Copyright © Scott Bradner & Ben Gaucherin 2015

Secure Servers, contd.



- Internet accessible servers should be stateless
No data stored on server
Data should be stored on backend server that is not addressable from Internet or most of corporate network
Should be a firewall between server and data server (in addition to firewall between server and Internet)

12

Copyright © Scott Bradner & Ben Gaucherin 2015

Secure Network Segments



- Router ACLs and firewalls should be used to restrict traffic into and out of important LAN segments
Default: deny all
Can be a problem because of software vendors that assume no outbound filtering
But required by PCI DSS
- Traffic using commonly exploited ports should be blocked to all LANs except where actually needed
i.e., do not have blanket exceptions to deny all default

13

Copyright © Scott Bradner & Ben Gaucherin 2015

Secure Communications



- Assume all communications can be overheard
- Assume wireless networks are insecure
Even with Wi-Fi security
Same with any network (including LAN) segments
- All ~~important~~ communications should be encrypted end-to-end
e.g., secure internet-facing servers (https, SSL, TLS)

14

Copyright © Scott Bradner & Ben Gaucherin 2015

WLAN Security



- Treat as all communications (encrypt end-to-end)
- First WLAN security was Wired Equivalent Privacy (WEP)
Poorly designed & easily broken - **not better than nothing**
- IEEE defined 802.11i to replace WEP
Quite good
Wi-Fi Alliance defined Wi-Fi Protected Access (WPA) based on 802.11i

15

Copyright © Scott Bradner & Ben Gaucherin 2015

Control Access to Network

- Restrict access to LAN (physical or wireless)
e.g., 802.1x
e.g., web redirection and MAC address registration
Can spoof MAC addresses, so not perfect
- But do not assume that systems on the company network are trusted just because they are on the company network

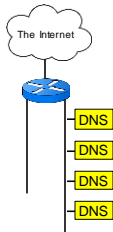


Whistleblowers are generally insiders

19

Copyright © Scott Bradner & Ben Gaucherin 2015

Know What You Did



- By maintaining an audit trail of all changes to access rules
Record who, when, what and why
Learn from Microsoft's DNS problems
For firewall rules and Access Control Lists in routers and switches
- So you can understand where all the rules came from a year later
And maybe know what rules should still be there

20

Copyright © Scott Bradner & Ben Gaucherin 2015

Ransomware



- Attacker encrypts your data and demands a ransom to give you the key to decrypt it
- Ransomware depends on two failures to succeed
 - 1/ failure of good security practices – e.g. failure to patch, clicking on bad URL, visiting bad web site
attacker needs a vulnerability to get access
 - 2/ failure to have good offline backups
restore from backup is a ransomware cure

21

Copyright © Scott Bradner & Ben Gaucherin 2015

Image credits

All drawings and photos by Scott Bradner unless noted

Slide#	credit
2	http://www.amazon.com/PNY-Turbo-25-6GB-Flash-Drive/dp/B00JN1TOHM
3	http://www.huffingtonpost.com/2013/05/17/facebook-user-numbers_n_3292316.html
4	http://www.firemon.com/advancing-firewall-necessary-evils-10-tuple/
5	http://solutions-institute.org/secure-communications-10-steps-to-encrypt-your-email/
6	http://www.thefullwiki.org/Lobster
9	http://itechjsc.com.vn/techsupport/dell/desktops/op960/sm/mt_speak.htm
10	http://www.esecurityplanet.com/network-security/computer-thefts-expose-over-45000-patients-personal-data.html

22

Copyright © Scott Bradner & Ben Gaucherin 2015

Image credits

All drawings and photos by Scott Bradner unless noted

Slide#	credit
11	http://www.sanderssoftware.com/solutions-virtualization.htm
12	http://www.servtelecom.com/te-disenamos-un-control-total-de-acceso-a-internet/
15	http://mile2.com/latest-news/how-to-crack-a-wep-key-step-by-step.html
16	http://www.itbusiness.ca/blog/4-questions-to-ask-when-establishing-a-byod-policy-for-your-business/20867
17	http://readwrite.com/2012/02/14/infographic-the-cost-of-stolen
18	https://vimeo.com/100545663
19	http://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline
21	https://optometrydivas.com/3-ways-to-protect-your-practice-from-ransomware-attacks/

23

Copyright © Scott Bradner & Ben Gaucherin 2015




Security fundamentals
Threat mitigation III: portable media and residual data on disk drives

CSCI E 45a: The Cyber World – part A

1 Copyright © Scott Bradner & Ben Gaucherin 2015

The Risks of Portable Media

- Portable media: very large capacity, very concealable & very easy to lose
For comparison, a 250 GB thumb drive would hold over 300 times the documents that Manning took.
- Insider threat small percent of overall threat but still significant
And that is only for purposeful incidents




Chelsea Manning official Army photograph

Verizon Breach Report

2 Copyright © Scott Bradner & Ben Gaucherin 2000

The Risks of Portable Media, contd.

- Even when an insider is not trying to sneak data out there is a worry
- The data comes along if someone steals the drive
E.g., military mission plans
- Issues:
Putting sensitive data on portable drives
Not encrypting the drives




Portable computer drives peddled at bazaar outside Bagram Air Base



3 Copyright © Scott Bradner & Ben Gaucherin 2005

The Risks of Portable Media, contd.



- Drives with embedded encryption are available
- Software on OS can encrypt drive
- Just do it!
- Same issue if drive is in portable device
E.g., a laptop or smartphone

Another breach in the data security wall; 2,700 exposed
By Jason Cole | February 4, 2015
Barclay Health Partners, a New York City based managed long-term care Medicaid and Medicare plan, has reported that 2,700 of its members have had their personal healthcare records stolen and possibly compromised.

The company, a subsidiary of HealthFirst, a New York health insurer, said on 2/3/15 that the personal data involving personal medical records on a smartphone and an encrypted laptop were compromised by a former HealthFirst, a business associate of Barclay Health Partners.

Encrypted records, but the key to break the encryption also was stolen in the laptop bag taken from the apartment, according to the statement.


Medical records

The personal data involved in the breach resided on a smartphone and an encrypted laptop computer stolen

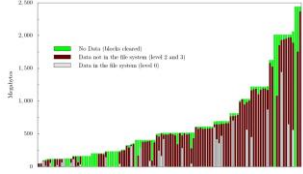
the key to break the encryption also was stolen in the laptop bag taken from the apartment,

4 Copyright © Scott Bradner & Ben Gaucher in 2015

Residual Data on Disk Drives



- Normal file removal and disk formatting commands do not actually remove data
Just removes pointers to data - disk forensics can recover




data still on used disks

green=OK
rest not OK

Simson Garfinkel

5 Copyright © Scott Bradner & Ben Gaucher in 2015

Residual Data on Disk Drives, contd.



- To actually overwrite data
Macs
"Secure Empty Trash" in Finder
"srm" in terminal
"Secure Erase" in Disk Utility
Windows
Norton & Symantec tools
Linux
srm
- Some tools may not work well with SSD drives
Tool must support "ATA Secure Erase"
Check the fine print

6 Copyright © Scott Bradner & Ben Gaucher in 2015

Residual Data on Disk Drives, contd.



- When done with disk drive –
Follow DoD 5220.22-M
“10 penny nail properly inserted”
Type 1 Degausser
Google finds many products & services
Drive slagging

7

Copyright © Scott Bradner & Ben Gaucherin 2015

Image credits

All drawings and photos by Scott Bradner unless noted

Slide# credit

2 <http://www.amazon.com/PNY-Turbo-256GB-Flash-Drive/dp/B00JN1TOHM>

Manning -

https://en.wikipedia.org/wiki/Chelsea_Manning

verizon - <http://www.verizonenterprise.com/DBIR/2015/>

3

http://www.nbcnews.com/id/12305580/ns/nbc_nightly_news_with_brian_williams-nbc_news_investigates/t/stolen-military-data-sale-afghanistan/

4 <http://www.computerworld.com/article/2879710/back-to-the-future-toshiba-touts-a-usb-flash-drive-with-keypad-passkey.html>

<https://skatter.com/2007/11/ironkey-encrypted-flash-drive-review/>

5 <http://www.cnetonline.com/news/60tb-disk-drives-could-be-a-reality-in-2016/>

6 <http://eecie.com/c/disk-slagger>

7


Copyright © Scott Bradner & Ben Gaucherin 2015

Security fundamentals
Threat mitigation IV: enterprise security policy

CSCI E 45a: The Cyber World – part A

1 Copyright © Scott Bradner & Ben Gaucherin 2015


Enterprise Security Policy

 Enterprise Security Policy

- An Enterprise Security Policy (ESP) is, normally, a set of high-level policies that addresses specific areas of security concern
But can be very detailed (see Mississippi's)
- Best developed by an effort involving stakeholders across the organization
So it does not seem to be just imposed

2 Copyright © Scott Bradner & Ben Gaucherin 2015

Enterprise Security Policy, contd.

 HARVARD Information Security

- All enterprises should have one
See www.security.harvard.edu for Harvard's
- Policy development is both art and science
And politics
- ESPs create an explicit set of standards for user behavior
Can't say "I didn't know"

3 Copyright © Scott Bradner & Ben Gaucherin 2015

How to Develop an ESP



Marc Gartenberg

- Know your organization
- Define scope and agenda
- Know your target audience
- Stay high-level, general and broad
- Must be easily translated into procedures & guidelines
- Keep organizational weakness in mind

Marc Gartenberg (Computerworld)

4

Copyright © Scott Bradner & Ben Gaucherin 2015

How to Develop an ESP, contd.



Shirley Chiang

- Be aware of external drivers
- Be realistic
- Use version control and backups
- Avoid controversy
- Wear a white hat
- Don't forget to smile & keep a sense of humor

Marc Gartenberg (Computerworld)

5

Copyright © Scott Bradner & Ben Gaucherin 2015

Image credits

All drawings and photos by Scott Bradner unless noted

Slide# credit

4 <http://www.slashgear.com/slashgear-welcomes-michael-gartenberg-0948914/>

5 <http://www.yeehawcowboy.com/Los-Altos-Hats-Joan-Style-Felt-Cowboy-Hat-4x-6x-10x-Available-Joan-brim-felt-cowboy-hat-1-13.htm>

<http://www.artshole.co.uk/shirleychiang.htm>

6


Copyright © Scott Bradner & Ben Gaucherin 2015

Security fundamentals
Conclusion


CSCI E 45a: The Cyber World – part A

1 Copyright © Scott Bradner & Ben Gaucherin 2015

Summary





- C.I.A. is a good way to think about information security
 - Confidentiality
 - Integrity
 - Availability
- Factoring in people makes security harder
- Secrecy ≠ security
- People do not understand risk well



Auguste Kerckhoffs

2 Copyright © Scott Bradner & Ben Gaucherin 2015

Summary, contd.



- 4 steps to risk analysis
 - 1 understand threats
 - 2 understand probability
 - 3 understand potential damage
 - 4 mitigate based on risk
- Risks to human life present special issues
- Stopping service may be warranted
- Attack trees are a logical approach
- Multiple possible mitigation areas

3 Copyright © Scott Bradner & Ben Gaucherin 2015

Image credits

All drawings and photos by Scott Bradner unless noted

Slide# credit

2 cia - <http://www.digitalthreat.net/2011/12/anti-virus-wont-keep-your-data-safe/>

kerkhoffs - <https://commons.wikimedia.org/wiki/File:Kerkhoffs.jpg>

3 face -

https://commons.wikimedia.org/wiki/File:Paris_Tuileries_Garden_Facepalms_statue.jpg

locks - <http://www.bbb.org/blog/2012/06/is-my-social-security-number-safe/>

4

Copyright © Scott Bradner & Ben Gaucherin 2015
