


Surveillance and counter-surveillance
Introduction

CSCI E 45b: The Cyber World – part B

1 Copyright © Scott Bradner & Ben Gaucherin 2016

Introduction: learning goals



- Understand the pervasiveness of surveillance
- Understand who is doing surveillance
- Understand the legal aspects of surveillance
- Understand the surveillance techniques
- Understand anti-surveillance possibilities
- Understand the impact of surveillance on society

2 Copyright © Scott Bradner & Ben Gaucherin 2016

Topics, all required



- Surveillance base
Context & players of surveillance
- Surveillance: laws
Some of the US laws relating to surveillance
- Surveillance: techniques
How is surveillance done?
- NSA surveillance
What we know the NSA has been doing

3 Copyright © Scott Bradner & Ben Gaucherin 2016

Topics, contd.



- Surveillance: non-government surveillance
Ad companies, ISPs, employers
- Surveillance and society
What is the impact of surveillance on society?
- Anonymity
What is it and who needs it?
- Privacy protecting technology
Encryption, steganography, mixers & proxies

4

Copyright © Scott Bradner & Ben Gaucherin 2016

Topics, contd.



- Onion routing and Tor
What is onion routing
How does Tor work?
What are the issues with Tor?

5

Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

Slide# credit

3 <https://www.quora.com/topic/Communications-Assistance-for-Law-Enforcement-Act-CALEA>

<https://www EFF.org/pages/eff-nsa-graphics>

4 <http://www.amatrixsoft.com/power-spy-software.php>

<http://techland.time.com/2012/05/24/the-new-york-bill-that-would-ban-anonymous-online-speech/>

5 <http://www.powworld.com/article/2848292/malware-served-through-rogue-tor-exit-node-tied-to-cyberespionage-group.html>

6


Copyright © Scott Bradner & Ben Gaucherin 2016

Surveillance & surveillance avoidance
Surveillance: introduction

CSCI E 45b: The Cyber World – part B

1 Copyright © Scott Bradner & Ben Gaucherin 2016

Surveillance





- Not just for spies and criminals anymore
- Surveillance by governments but also surveillance by others
e.g., spyware, industrial espionage, browsing habits, ...

sur·veil·lance |sarvə'ləns|
noun
close observation, esp. of a suspected spy or criminal : *he found himself put under surveillance by military intelligence.*

ORIGIN early 19th cent.: from French, from *sur-* 'over' + *veiller* 'watch' (from Latin *vigilare* 'keep watch').

2 Copyright © Scott Bradner & Ben Gaucherin 2016

Physical and cyberworld surveillance



- Surveillance is much easier in the cyberworld
- Reading every letter or following every person not feasible in the physical world – easy in the cyberworld
- Some legal limits on physical surveillance
Use of thermal detectors
Use of dope sniffing dogs
- Legal limits in cyberspace being worked out

3 Copyright © Scott Bradner & Ben Gaucherin 2016

Example cyberworld players



- National Security Agency (NSA): government actor
Dual mission:
 - Signals Intelligence (SIGINT): spying on communications and information systems
 - Information Assurance: protect US national security systems and dataEvery country has such actors

4

Copyright © Scott Bradner & Ben Gaucherin 2016

Example cyberworld players, contd.



Surveillance Marketing

- Google & other ad companies
Develop understanding of the interests of Internet users to better deliver ads that the users will respond to
Hundreds of ad & other companies track users
Database-driven marketing - database of surveillance results
A "big data" opportunity

5

Copyright © Scott Bradner & Ben Gaucherin 2016

Example cyberworld players, contd.

Snap and save up to 30% more.



You have zero privacy anyway. Get over it.
Scott McNealy 1999

- Service providers
 - Cellular telephone companies
 - GPS direction services
 - Car rental companies
 - Insurance companies
 - Transit authorities
 - Credit card companies
- Private players: crooks, idealists, spouses, ...

6

Copyright © Scott Bradner & Ben Gaucherin 2016

Anti-Surveillance



- Designing systems so that surveillance is hard(er)
- Using technology to hide communications
- Hiding secrets in communications

7

Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

Slide#	credit
2	https://commons.wikimedia.org/wiki/File:Google_2015_lo_go.svg https://commons.wikimedia.org/wiki/File:National_Security_Agency.svg
3	http://blog.modernmechanix.com/what-happens-when-you-mail-a-letter/ http://www.dailymail.co.uk/news/article-2120626/House-hiding-cannabis-factory-captured-helicopter-police-thermal-imaging-camera.html
4	https://commons.wikimedia.org/wiki/File:National_Security_Agency.svg
5	https://commons.wikimedia.org/wiki/File:Google_2015_lo_go.svg
6	http://www.yourinsurancecompany.com/automobile/progressive_snAPSHOT_informatio
n.aspx	http://events.r20.constantcontact.com/register/event?eidk=a07e5wpnfhu6e4ec88d8&rsqwr7cab
7	https://en.wikipedia.org/wiki/Tor_%28anonymity_network%29#Hidden_services

8


Copyright © Scott Bradner & Ben Gaucherin 2016

Surveillance & surveillance avoidance
Surveillance: laws

CSCI E 45b: The Cyber World – part B

1 Copyright © Scott Bradner & Ben Gaucherin 2016


CALEA



- *Communications Assistance for Law Enforcement Act*
- Rules on what telecommunications carriers must be able to do if they receive a subpoena
 - Has no impact on what a subpoena can ask for
 - i.e., a subpoena can ask for things that CALEA does not require a carrier to be able to do
 - Carrier has to do what they are able to do

2 Copyright © Scott Bradner & Ben Gaucherin 2016

National Security Letters



- Way to get info on the subject of an investigation w/o a subpoena
 - No judicial oversight
- Recipient not permitted to disclose NSL
- Most use since USA PATRIOT Act
 - 143,074 NSLs by FBI in two year period (ACLU)
 - 53 criminal referrals (0 for terrorism) – 0.037%
 - 17 money laundering, 17 immigration, 19 fraud

3 Copyright © Scott Bradner & Ben Gaucherin 2016

[Slide content removed]

- The content of this slide was superseded by later events, and has been removed.

4

Copyright © Scott Bradner & Ben Gaucherin 2016

U.S. Wiretap Act

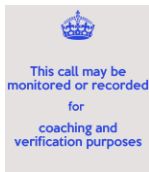


- Prohibits purposeful interception, disclosure or use of wire, oral or electronic communication through the use of a device
- Exceptions:
 - Consent by a party to the communications
 - State law may require all parties to agree
 - Provider self defense
 - Computer trespasser
 - Directed by law enforcement

5

Copyright © Scott Bradner & Ben Gaucherin 2016

U.S. Wiretap Act: Consent



- Requires “prior consent”
 - Can be part of employment conditions
 - Employer can claim ownership of all communications using company equipment of networks
 - Can be in terms of service
 - Service provider can state that user can not expect privacy
 - Can be in a banner
 - “This call may be monitored to improve service”

6

Copyright © Scott Bradner & Ben Gaucherin 2016

U.S. Wiretap Act: Provider Protection

Volume 6, Number 2, Spring 1995
AN AFFRONT TO HUMAN DIGNITY: ELECTRONIC MAIL MONITORING IN THE PRIVATE SECTOR WORKPLACE
 Larry D. Newman, Jr.
 "Cases and controversies over the draft of Title VII of the program of the human code... (3) and discretion are made... consultation must address also... and long past with the code."
INTRODUCTION
 Although employers have historically monitored their employees, the common widespread development of sophisticated technology is greatly increasing the amount and type of information available to those employers. How do we respond? An early technological affront was discussed in a paper published in the November of the work environment, which makes reference to monitoring "electronic surveillance." For instance, in

Harvard Journal of Law and Technology - Spring 1995

- OK to monitor to protect "the rights of property of the provider"
 Issue if this excuse is used to provide real time info to law enforcement
 But if records of prior proper monitoring exist then information can be provided to law enforcement
- Provider can not act as an agent of law enforcement w/o subpoena

U.S. Wiretap Act: Computer Trespass

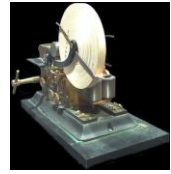
(A) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and (B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer.
 Wiretap Act

- Law enforcement can intercept traffic from "computer trespassers"
 "Computer trespasser" anyone who does not have existing agreement with provider to use computer
 Everyone has implied agreement allowing access to information that is made public
- Only if authorized by provider

Types of Wiretaps in U.S.



AI may soon eliminate requirement for monitoring by a human



Telegraph Pen Register

- Non-real time
 Call records normally maintained by phone company
 Law enforcement collects this information from carriers
- Real time
 Pen register: record numbers called by target phone
 Trap and trace: record numbers that called a target phone
 Title III: record contents of calls - non-relevant calls must be "minimized" - requires live monitoring

Types of Wiretaps in U.S., contd.



- Does not cover stored communications
Covered by Electronic Communications Privacy Act of 1986

10

Copyright © Scott Bradner & Ben Gaucherin 2016

Councilman Case



- Bradford C. Councilman ran Interloc, an on-line rare book listing service and also provided email accounts to book dealers
- Email service made copies of email to book dealers from Amazon for Councilman to read
- Arrested and charged with violating Wiretap Act

11

Copyright © Scott Bradner & Ben Gaucherin 2016

Councilman Case



Judge Lipetz, dissented

- Councilman claimed that email was in temporary storage, not in transit, thus not subject to the Wiretap Act
- District court and 3-judge panel of Appeals court agreed and dismissed charge (by a vote of 2-1)

12

Copyright © Scott Bradner & Ben Gaucherin 2016

Councilman Case, contd.



- Decision gutted Wiretap Act when it came to digital communications because packets are in storage in a router before being forwarded

A fact mentioned in the decision

13

Copyright © Scott Bradner & Ben Gaucher in 2016

Councilman Case, contd.



Judge Lipez, wrote majority decision

- Full Appeals Court panel reconsidered and reversed the previous decision (by a vote of 5-2)

Temporary storage not exempted from Wiretap Act

- Councilman retried in Feb 2007 & acquitted

Jury was not convinced that the redirection had happened

14

Copyright © Scott Bradner & Ben Gaucher in 2016

Privacy of Email



- Government argues that users have no reasonable expectation of privacy for email stored at a email service provider
e.g., Google "reads" the mail to target ads
- Also, Electronic Communications Privacy Act says no warrant needed for info stored more than 180 days

15

Copyright © Scott Bradner & Ben Gaucher in 2016

Privacy of Email, contd.



- U.S. Appeals Courts have split on need for a court order to get older email messages
Supreme Court declined to clarify
– April 15 2013
Looking for a cleaner case?

16

Copyright © Scott Bradner & Ben Gaucherin 2016

Tracking Movement



- Supreme Court ruled that law enforcement needs to get a warrant before installing a GPS tracker
Unanimous, but confused ruling
Sotomayor's consent opinion suggested need to review basic assumptions in light of technology changes
No such restriction for private parties
4th Amendment does not apply to private parties
some state laws prohibit GPS tracking of people

17

Copyright © Scott Bradner & Ben Gaucherin 2016

Tracking Movement, contd.



- Same information available from:
Cell phone records
Car navigation systems
Car help systems
- No court guidance on accessing those records

18

Copyright © Scott Bradner & Ben Gaucherin 2016

Physical imitations required

- Thermal checking & dog sniffing for Marijuana



cannabis factory in England

19

Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

Slide#	credit
2	https://www.quora.com/topic/Communications-Assistance-for-Law-Enforcement-Act-CALEA
3	http://www.cnet.com/news/google-offers-data-on-fbis-national-security-related-requests-for-user-identities/
4	https://www.dfi.org/press/logs
5	https://www.timeline.com/stories/bootleggers-big-dat-a-wiretapping-america
6	http://www.keepcalm-o-matic.co.uk/p/this-call-may-be-monitored-or-recorded-for-coaching-and-verification-purposes/
7	http://pol.law.harvard.edu/articles/pdf/v08/08HarvLTech345.pdf
9	https://nedsincourt.wordpress.com/2013/06/11/on-prism-smith-and-pen-registers/
10	http://opus4idels.com/insights/google-and-yahoo-prepare-to-defy-the-electronic-communications-privacy-act/
11	http://www.trademarkia.com/interloc-73431810.html
12 & 14	http://newenglandinhouse.com/2013/11/05/2218/
15	https://commons.wikimedia.org/wiki/File:Google_2015_Logo.svg
16	https://commons.wikimedia.org/wiki/File:Seal_of_the_United_States_Supreme_Court.svg
17	http://www.beagrdnews.com/2014/08/frost-might-need-gps-tracker/
5011718	http://www.mirror.co.uk/news/real-life-stories/my-husband-spies-smartphone-app-5011718
18	http://www.autoguide.com/buyers-guide/automotive-gps-navigation-guide-1106.html
	http://mediagm.com/onstah.html
19	http://news.bbc.co.uk/2/hi/uk_news/magazine/7412654.stm
20	Copyright © Scott Bradner & Ben Gaucherin 2016

Surveillance & surveillance avoidance
Surveillance: techniques

CSCI E 45b: The Cyber World – part B

1 Copyright © Scott Bradner & Ben Gaucherin 2016

Surveillance: Eavesdropping

- Eavesdropping at source or destination
e.g., listening to audio, observing display or keyboard
- Audio bugs
Electronic bugs can be detected
Remotely enable telephones & PC mikes & cameras
- Directional microphones
Post process signals to
Eliminate background noise
- Bounce laser off windows
“See” vibrations

2 Copyright © Scott Bradner & Ben Gaucherin 2016



Surveillance: Emissions Security (EmSec)

- Desire: to capture information in transmission or processing
- Crosstalk on telegraph wires monitored in 1880s
- Leakage from telephone wires monitored by 1914
- Monitor photons escaping from optical fibers
Reports: U.S.S. Jimmy Carter can tap undersea fiber cables

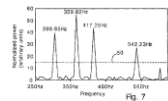
3 Copyright © Scott Bradner & Ben Gaucherin 2016



optical fiber identifier
Noyes Fiber Systems



Passive Emissions-Based Attacks



U.S. Patent No. 7,877,621
Detecting software attacks
by monitoring electric
power consumption
patterns

- Power consumption patterns
Different processor instructions consume different amounts of power
Used by governments & researchers
Counter by adding non-relevant processing

4

Copyright © Scott Bradner & Ben Gaucherin 2016

Passive Emissions-Based Attacks



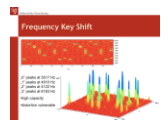
Markus Kuhn: demo
at CEBIT 2006 -
from 25 m

- RF signals from equipment & cables
e.g., monitor RF from video display to determine what is being displayed
Counter by adding RF shielding
Also works with flat panel displays (including laptops)

5

Copyright © Scott Bradner & Ben Gaucherin 2016

Active Emissions-Based Attacks



Tempest virus used to transmit
device passwords from tablet

- “tempest virus”
Introduce program to create RF broadcasts of sensitive information
- Put transmitter near processor
e.g., cell phone output modulated by processor activity
- Glitch power supply
Can cause processing errors that can be exploited

6

Copyright © Scott Bradner & Ben Gaucherin 2016

Emissions-Based Attacks: Relevance

The EM Side-Channel(s) Attacks and Assessment
Methodologies
Shakil Agrawal, Bruce Arbaugh, and Srinivas S. Bala
IBM Research
IBM Watson Research Center
201 N. York Ave.
Yorktown Heights, NY 10598
email: {sagrawal, arbaugh, bala}@us.ibm.com

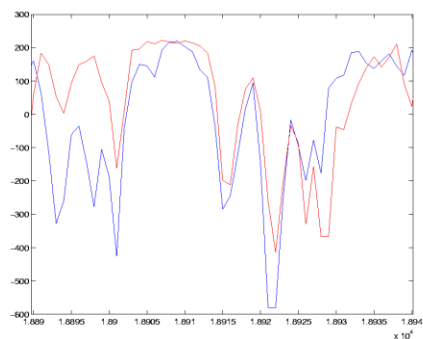
Abstract
We present a novel side-channel attack on the order of instructions in a processor. The attack is based on the observation that the power consumption of a processor is sensitive to the order of instructions. We show that the power consumption of a processor is sensitive to the order of instructions. We show that the power consumption of a processor is sensitive to the order of instructions. We show that the power consumption of a processor is sensitive to the order of instructions.

- Example from IBM researchers
Agrawal, Archaubeault, Rao & Rohatgi
Monitor emissions from a processor
Compare multiple program runs
Can isolate instructions and data
Key off of power consumptive instructions

7

Copyright © Scott Bradner & Ben Gaucherin 2016

Tested Bit Same in Two Runs

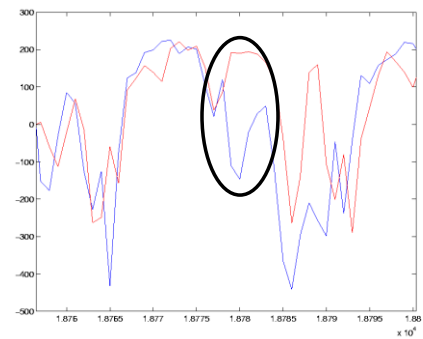


Agrawal et al

8

Copyright © Scott Bradner & Ben Gaucherin 2016

Tested Bit Different in Runs



Agrawal et al

9

Copyright © Scott Bradner & Ben Gaucherin 2016

Anti-Surveillance: TEMPEST



- Aims at eliminating equipment emissions that could be used to disclose information
Radio & light emissions as well as power consumption
- Mostly classified US government program
Classified in 1970s
Some public research in mid '80s and '90s
- Standards to minimize emissions and certification programs

10

Copyright © Scott Bradner & Ben Gaucherin 2016

US Army TEMPEST Test Facility



Electronic Proving Ground

EMI, EMC, & TEMPEST Test Facility



• Secure Compound

• RF-Isolated Area

• Fully portable measurement equipment

• Seven shielded chambers

• Anechoic, 120dB isolation

• Semi-anechoic, 100dB isolation

• One Transverse Electromagnetic/Reverberation chamber



• 10 Hz - 40 GHz instrumentation suites

• NARTIE and NSA certified Engineers

• EMI/EMC, TEMPEST testing and technical consulting services

• Instrumented to test to all military MIL-STD and C3 requirements, with capabilities to meet many civilian requirements



— Roadlines Through Testing —

[Back to Facilities Page](#) 9

11

Copyright © Scott Bradner & Ben Gaucherin 2016

Sound too



Extract RSA key by analyzing high-frequency noise emitted by computer processing encrypted chosen cyphertexts

Using cellphone placed next to laptop or directional microphone 4m away
Same technique applies to measuring the electric potential of a computer chassis.

12

Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

Slide#	credit
2	https://commons.wikimedia.org/wiki/File:NSA_Great_Seal_bu.jpg http://www.professorwalter.com/2009/11/be-careful-what-you-say-someone-may-be-listening.html
	http://godardfanforever.tumblr.com/post/90399096723/working-on-some-70s-paranoiaconspiracy-thrillers
3	http://www.photonics.com/m/Company.aspx?CompanyID=397&PRID=49297 http://www.1001modelkits.com/submarines/modelkits/17383-hobby-boss-87004-uss-jimmy-carter-ssn-3-submarine-submarines-6939319270047.html
4	Figure 7 from U.S. Patent No. 7,877,621
5	https://www.newsident.com/blog/technology/2007/04/seeing-through-walls.html
6	http://www.forensics-research.com/index.php/projects/windows-mobile-estimated-virus/
7, 8 & 9	https://www.cs.jhu.edu/~astubble/600.412/s-c-papers/em.pdf
10	http://hackaday.com/2015/10/19/tempest-a-tin-foil-hat-for-your-electronics-and-their-secrets/
11	www.epgarmy.mil/e3tf.aspx
12	https://www.tau.ac.il/~tromer/papers/acoustic-20131218.pdf

13

Copyright © Scott Bradner & Ben Gaucherin 2016

Surveillance & surveillance avoidance
Surveillance: NSA surveillance

CSCI E 45b: The Cyber World – part B

1 Copyright © Scott Bradner & Ben Gaucherin 2016

National Security Agency




Harry Truman

- Roots during World War I
Cipher Bureau and Military Intelligence Branch, Section 8 (MI-8)
- Current NSA formally established by President Truman in 1952
- Dual mission:
 - Protect US communications infrastructure
 - Eavesdrop on communications of other countries

2 Copyright © Scott Bradner & Ben Gaucherin 2016

NSA dual mission



- Missions in conflict
 - Protecting mission wants better cryptography
 - Eavesdropping mission wants to break cryptography
- Until early 2016 missions were separate within NSA – now merged

3 Copyright © Scott Bradner & Ben Gaucherin 2016

Precursor?



John Ponder

- Total Information Awareness (TIA): started in DARPA in 2002
 - Mechanism: gather all possible information about everybody
 - Not just communications
 - Goal: find terrorists
- Officially killed by congress in late 2003
 - Seemed to be dead
- Data gathering desire lived on

4

Copyright © Scott Bradner & Ben Gaucher in 2016

NSA surveillance—the recent past



Edward Snowden

- Pre-Snowden
 - Assumed that governments collected information about specific people or groups for specific reasons
 - Even when not waiting for a court order
- Post-Snowden
 - Now know that at least the NSA wants to gather all information it can about everybody “big pipe”
 - Claims to only look at the data about specific people after there is a specific reason to do so

5

Copyright © Scott Bradner & Ben Gaucher in 2016

NSA information gathering



- (All) phone call metadata (U.S. and elsewhere)
 - The law changed post Snowden
- Non-US phone calls
 - Including foreign leadership phone calls
- Examine most U.S. Internet traffic looking for “foreign intelligence”, keep copies of encrypted traffic
- Inter-data center traffic (Google, Yahoo!, ...)

6

Copyright © Scott Bradner & Ben Gaucher in 2016

NSA information gathering, contd.



- Contact lists (Yahoo!, Microsoft mail, Facebook, gmail, ...)
- Google search terms
- UN & foreign embassy communications
- ∞

7

Copyright © Scott Bradner & Ben Gaucherin 2016

NSA Programs



ECHELON from 2000 news story



PRISM logo?

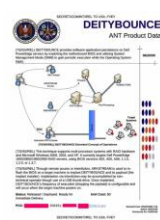
- Pre-2001
Echelon, Main Core, Minaret, Shamrock, Promis
- 2001
Blarney, Ragtime, Turbulence, Pinwale, Mainway, Upstream
- 2007
PRISM, Boundless Informant, X-Keyscore, Dropmire, Fairview, Surveillance Detection Unit, Bullrun, . . .

Wikipedia – review them on Wikipedia

8

Copyright © Scott Bradner & Ben Gaucherin 2016

NSA, other activities



ANT catalog

- Subvert security standards
- Has backdoors for many types of equipment
50 page “catalog” by NSA’s ANT group
Advanced (or Access?) Network Technology
Part of Tailored Access Operations unit (TAO)
NSA hacking operation Exposed by DER SPIEGEL

9

Copyright © Scott Bradner & Ben Gaucherin 2016


NSA, in theory



- Can collect and do anything it wants to with any information about non-US persons
- Can only look at data on specific US persons if authorized by a court
Including the secret Foreign Intelligence Surveillance (FISA) Court

10 Copyright © Scott Bradner & Ben Gaucher in 2016

NSA, in theory



- But the NSA interpreted the rules to mean that it can collect any information it wants to about everyone (including US persons)
But not look at the data unless it has a specific reason
Which it can get retrospectively authorized by the FISA court
- Law changed in 2015
NSA can no longer directly collect bulk telephone metadata
Must get records for specific targets from phone companies

11 Copyright © Scott Bradner & Ben Gaucher in 2016

International cooperation



- Intelligence agencies around the world cooperate with the NSA
- Some have been doing so for a long time
E.g., ECHELON (a.k.a., The Five Eyes) (Australia, Canada, New Zealand, the United Kingdom, and the United States) spy on each other's citizens for each other since the 1960s (and to bypass national legal restrictions)

Five Eyes

NSA now says that they are not permitted to do this



12 Copyright © Scott Bradner & Ben Gaucher in 2016

International cooperation



- Close cooperation with the Government Communications Headquarters (GCHQ) – England
Signals intelligence agency started after WW 1

13

Copyright © Scott Bradner & Ben Gaucherin 2016

NSA, flawed trade-off analysis



Angela Merkel



Edward Snowden

- Apparently NSA never considered the possibility of an insider threat
i.e. that someone inside would expose their activities
- Thus the cost-benefit analysis was flawed
e.g. the downsides of exposure of tapping the German President's personal phone were not considered
- Also, no contingency plans for what to do if activities were exposed

14

Copyright © Scott Bradner & Ben Gaucherin 2016

NSA surveillance and the Katz case

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized" – 4th Amendment

- The Katz case relied on the concept of a "reasonable expectation" of privacy
The Supreme Court's attempt to define "unreasonable"
- Snowden changed the playing field
Now that we know the NSA is watching is it possible to have a "reasonable expectation" that they are not?

15

Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

Slide#	credit
2	truman
3	https://en.wikipedia.org/wiki/National_Security_Agency
4	https://en.wikipedia.org/wiki/Total_Information_Awareness
5	http://www.globalresearch.ca/one-year-of-edward-snowdens-revelations/5385902
6	https://www.eff.org/pages/eff-nsa-graphics
7	https://commons.wikimedia.org/wiki/File:Yahoo!_logo.svg http://logos.wikia.com/wiki/Outlook.com https://commons.wikimedia.org/wiki/File:Google_2015_logo.svg
8	http://www.bibliotecapleyades.net/ciencia/maganes/ech_ebn07_15.jpg
9	https://www.eff.org/files/2014/01/06/20131230-appelbaum-nsa_ant_catalog.pdf
10	http://www.iftennis.com/procircuit/tournaments/organisers-info/application-pack-usa.aspx
11	http://www.fiscuscourts.gov/ http://www.zmescience.com/ecology/world-population-doubles-04325235/ http://judiciary.house.gov/index.cfm/us-a-freedom-act
12	https://en.wikipedia.org/wiki/Five_Eyes#/media/File:UKUSA_Map.svg
13	https://en.wikipedia.org/wiki/Government_Communications_Headquarters
14	https://www.youtube.com/watch?v=5YakmVt94HA http://www.globalresearch.ca/one-year-of-edward-snowdens-revelations/5385902

16

Copyright © Scott Bradner & Ben Gaucherin 2016

Surveillance & surveillance avoidance
Surveillance: non-government surveillance

CSCI E 45b: The Cyber World – part B

1 Copyright © Scott Bradner & Ben Gaucherin 2016

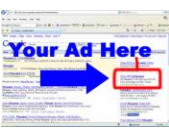
Non-Government Surveillance



- Internet is “free” for most applications
- Not actually free - you are exposed to advertisements and are expected to buy things

2 Copyright © Scott Bradner & Ben Gaucherin 2016

Non-Government Surveillance



- >100 ad companies & ad networks track Internet usage – Google is best known, but not alone
- Can link to other information sources – e.g. credit cards
- Aim of tracking: serve ‘more relevant’ advertising
- Assume that everything you do on-line is monitored & recorded
- And obtainable by governments (and divorce lawyers)

Amazon Associates
ChartBeat
ClickTail
Criteo
DoubleClick
KruX Digital
Native
NetRatings SiteCensus
Omniure
Optimizely
Outbrain
SOASTA mPulse
Usabilla
Visual Revenue

35 trackers on usatoday.com Jan 2024

UPDATED

cntr.com trackers 1/2/15

3 Copyright © Scott Bradner & Ben Gaucherin 2024

ISP Spying

AT&T tracks "the webpages you visit, the time you spend on each, the links or ads you see and follow, and the search terms you enter... AT&T Internet Preferences works independently of your browser's privacy settings regarding cookies, do-not-track, and private browsing. If you opt-in to AT&T Internet Preferences, AT&T will still be able to collect and use your Web browsing information independent of those settings."



4

Copyright © Scott Bradner & Ben Gaucher in 2004

- AT&T records everything you do over their Gigapower fiber-based internet service \$29 (per AT&T, maybe as much as \$66) per month to opt-out
- Verizon adds "supercookie" string to smartphone URLs Can be used to track all web activity You can, in theory, opt out
- Where is net neutrality when we need it?

Employer Spying

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized" – 4th Amendment

5

Copyright © Scott Bradner & Ben Gaucher in 2006

- In US, employer can spy on employees almost without limit
Particularly if mentioned in employee manual
The 4th Amendment does not apply to private parties
- As long as not doing so at the request of the government
Government must use same process as for a person's home
Can get permission from employer
Can get permission from co-worker

Employer Spying, contd.



6

Copyright © Scott Bradner & Ben Gaucher in 2004 powerspy.com

changed name or went out of business

Computer spy software records Facebook use, all keystrokes typed, captures all incoming and outgoing 3Fs in Skype. It records all websites visited, emails read, documents opened, windows opened, clipboard activities, passwords typed and applications executed. Computer spy software even takes screen snapshots at your set interval like a surveillance camera, this may include popular instant messenger like Facebook Messenger, WhatsApp, Skype, Hangouts, Tinder, Viber, Telegram, LINE, google Talk, Yahoo Messenger and more.

- Many spy products in the marketplace
Some installed on a PC
Some monitor network
- Note that archiving of email and IM is required by regulation in some businesses
e.g., brokerage houses

Image credits

Slide#	credit
2	http://adage.com/article/adages/b-alti-more-sun-home-page-ad-turns-back-online-ad-clock/243838/
3	http://business-tips.net/advertising-at-the-foot-of-internet.html
4	http://arstechnica.com/information-technology/2015/03/atts-plan-to-watch-your-web-browsing-and-what-you-can-do-about-it/ https://commons.wikimedia.org/wiki/File:Verizon_logo.svg
5	
6	http://www.amatrixsoft.com/power-spy-software.php http://www.amatrixsoft.com/products.php

7


Copyright © Scott Bradner & Ben Gaucherin 2016

Surveillance & surveillance avoidance
Surveillance and society

CSCI E 45b: The Cyber World – part B


1 Copyright © Scott Bradner & Ben Gaucherin 2016

Society & surveillance



Werner Heisenberg

- Heisenberg principle
Observing a system can change the system
- What is the effect on society of ubiquitous surveillance?




Franz Kafka

- Note: it is illegal for US government employees to look at the documents that Snowden leaked

2 Copyright © Scott Bradner & Ben Gaucherin 2016

Is Surveillance, By Itself, Harmful?



- Government says: no harm, no foul
Also said, we won't tell you what we are doing, so you can not tell if there is harm – Snowden changed this

3 Copyright © Scott Bradner & Ben Gaucherin 2016

Is Surveillance, By Itself, Harmful?



Neil Richards

- Neil Richards says “yes”
 - A - Surveillance Transcends the Public-Private Divide
 - B. Secret Surveillance Is Illegitimate
 - C. Total Surveillance Is Illegitimate
 - D. Surveillance Is Harmful

“surveillance — covert and overt, public and private — menace our intellectual privacy and the processes of belief formation on which a free society depends”

4

Copyright © Scott Bradner & Ben Gaucherin 2016

Also, times change



Joe McCarthy



J. Edgar Hoover

- What once was benign became treacherous
- What was once an expression of protected political opinion became a career terminating discovery

AMERICANS
DON'T PATRONIZE REDS!!!!
YOU CAN DRIVE THE REDS OUT OF TELEVISION, RADIO AND HOLLYWOOD
THIS TRACT WILL TELL YOU HOW.
WHY WE MUST DRIVE THEM OUT.
1) The REDS have made our Screen, Radio and TV Moscow's most effective Fifth Columns in America . . .

5

Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

Slide#	credit
2	https://simple.wikipedia.org/wiki/Wern_Heis_enberg http://www.biography.com/people/franz-kafka-9359401
3	http://articles.baltimoresun.com/2013-06-18/news/bs-ed-horsey-big-brother-20130618_nsa-big-brother-national-security-agency
4	https://intellectualprivacyblog.wordpress.com/
5	http://genius.com/2718964 http://www.biography.com/people/j-edgar-hoover-9343398 https://en.wikipedia.org/wiki/Hollywood_blacklist

6


Copyright © Scott Bradner & Ben Gaucherin 2016

Surveillance & surveillance avoidance
Anonymity

CSCI E 45b: The Cyber World – part B

1 Copyright © Scott Bradner & Ben Gaucherin 2016



Anonymity



- (Of a person) *“not identified by name”*
Ability to communicate without being identified
- Anonymity protected *in political discussions* by the US Constitution

2 Copyright © Scott Bradner & Ben Gaucherin 2016

Anonymity



- Who needs anonymity?
 - Dissidents
e.g., those expressing unpopular political views
 - Whistleblowers
e.g., those exposing corporate or government wrongs
 - Journalists
e.g., communicating with unauthorized sources
 - Chat room participants for sensitive topics
e.g., AIDS help line, spousal abuse survivors

3 Copyright © Scott Bradner & Ben Gaucherin 2016

Who Needs Anonymity?, contd.



the man had been discussing his plans with an undercover federal informant when he was arrested



- Law enforcement
 - e.g., communicate with sources & undercover agents
- Governments
 - e.g., data gathering, communicate with agents
- You
 - e.g., looking at porn web sites
- Criminals
 - e.g., child porn sellers, drug sellers, extortionists, terrorists

Criminals & Anonymity

SILK ROAD CREATOR ROSS ULBRICHT SENTENCED TO LIFE IN PRISON



- Criminals already strive for anonymity
 - They are well motivated
- Making anonymity hard to get in order to expose criminals will mostly impact other uses
 - Since the criminals will use anonymity anyway
- But it's a balance

Anonymity from Whom?

- Type of anonymity needed depends on situation
 - Sender anonymous to message recipient
 - Need path anonymity
 - Recipient anonymous to message sender
 - Need path anonymity
 - Sender & recipient anonymity to observer
 - Need channel anonymity
- Who is it from?**
- Who is it going to?**
- Hide from Big Brother**

Image credits

Slide#	credit
2	http://techland.time.com/2012/05/24/the-new-york-bill-that-would-ban-anonymous-online-speech/
3	http://www.businessinsider.com/yahoo-denies-collaborating-with-iranian-government-2009-10
4	http://corruptauthority.com/bid-rigging-fbi-corruption-illegal-politicians-fraud-whistleblower-suit-filed-against-detroit-for-corrupt-building-department/ http://ifelines.co.za/ads-help-line-addressing-hiv-and-aids/
5	http://www.bustle.com/articles/133037-ny-man-planned-terrorist-attack-for-new-years-eve-in-order-to-pledge-allegiance-to-isis http://silkroad4drugs.org/silkroad-2-0-url/?utm_referrer=https%3A%2F%2Fwww.google.com
5	http://www.wired.com/2015/05/silk-road-creator-ross-ubricht-sentenced-life-prison/

7

Copyright © Scott Bradner & Ben Gaucherin 2016

Surveillance & surveillance avoidance
Privacy protecting technology

CSCI E 45b: The Cyber World – part B

1 Copyright © Scott Bradner & Ben Gaucherin 2016

Encrypt Communications

The quick brown fox jumped over the lazy dog

↓

E

↓

r{_OSG;{hnp6fM#
 +!_If;U>&TCbVVec
 WGclMZbr!

↓

D

↓

The quick brown fox jumped over the lazy dog

- **Encrypt specific information before sending**
 e.g., encrypt files before emailing them

Advantages:
 Can be done by end users

Disadvantages:
 Observers know you are protecting info
 Users know key(s)
 May be coerced into disclosing them
 Keystroke logger on source or destination can reveal keys

2 Copyright © Scott Bradner & Ben Gaucherin 2016

Encrypt Communications, contd.

IAB Statement on Internet Confidentiality

In 1998, the IAB and EFF concluded that the growth of the Internet depended on open, free communication. For the Internet to continue to grow, Internet communication must remain confidential. This means that the information that is sent over the Internet must be protected from unauthorized interception and disclosure. Encryption is the best way to protect this information. Encryption should be used to protect all sensitive information that is sent over the Internet. Encryption should be used to protect all sensitive information that is sent over the Internet. Encryption should be used to protect all sensitive information that is sent over the Internet.

The IAB now believes it is important for protocol designers, developers, and operators to make encryption the norm for Internet traffic.

- **Main disadvantage; observer knows who is communicating**
 Even if not know what is being said
- **Issue because secure communications not the normal case for applications such as email**
 If everybody used postcards for normal mail these sealed envelopes would seem suspicious

3 Copyright © Scott Bradner & Ben Gaucherin 2016

Hide Communications, contd.

Before Watermarking



After Watermarking

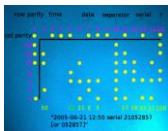
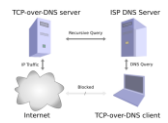


- Multiple techniques
e.g., manipulate low order bit of pixel information
Scatter message across image "randomly"
- Hidden watermarks are a type of steganography

7

Copyright © Scott Bradner & Ben Gaucherin 2016

Steganography, contd.



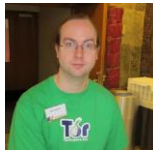
- Hundreds of steganography tools online
E.g. tunnel data over DNS
- Some experts think that is unlikely there is much use
Schneier: "easier to suck the data off onto a USB thumb drive"
- Printer serial numbers hidden in prints
using yellow dots

8

Copyright © Scott Bradner & Ben Gaucherin 2016

Hide Sender &/or Recipient

- Two example methods:
Use a "mix"
Use proxies



Roger Dingledine

Some of the following content is from Roger Dingledine

9

Copyright © Scott Bradner & Ben Gaucherin 2016

Mix

- Randomly decrypts & permutes inputs

10 Copyright © Scott Bradner & Ben Gaucherin 2016

Mix, contd.

- Mix function - observer can not determine which output came from which input

11 Copyright © Scott Bradner & Ben Gaucherin 2016

Mix Operation

12 Copyright © Scott Bradner & Ben Gaucherin 2016

Proxy-Based

- Messages appear to come from proxy instead of original sender
- Can be used for anonymous web browsing
- Multiple services on net
- Disadvantages: single point of failure, attack &

13 Copyright © Scott Bradner & Ben Gaucherin 2016

Psiphon

- Open source https web proxy
- Idea is to have lots of people set up proxies
- Free download of proxy software
- Users login, so user is not anonymous to proxy operator
- Operator only creates accounts for trusted parties
- Assumption: bad guys do not get accounts or run servers
- Started at the University of Toronto
- Funded by Open Society Institute (Soros Foundation)

14 Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

Figures by Scott Bradner unless noted

Slide#	credit
3	https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality/
4	https://www.ietf.org/rfc/rfc435.txt
	https://phpmatters.com/best-drupal-security-modules/
5	http://www.linuxjournal.com/article/9916
6	http://www.themakeupgalleryinfo.com/serious/taatto/rushhour3.htm
7	https://matlabprojects.org/security-projects/watermarking-projects/
8	http://analogbit.com/2008/07/27/tcp-over-dns-tunnel-software-howto/
	https://w2.eff.org/Privacy/printers%20color/
9	http://technical.ly/person/roger-dingledine/
10 - 12	Roger Dingledine
14	https://psiphon3.com/en/index.html
	http://psiphon.anuptodown.com/

15 Copyright © Scott Bradner & Ben Gaucherin 2016

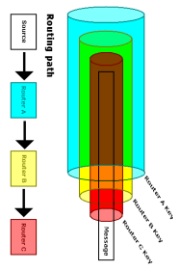
Surveillance & surveillance avoidance
Onion routing and Tor Concepts

CSCI E 45b: The Cyber World – part B

1

Copyright © Scott Bradner & Ben Gaucherin 2016

Onion Routing




- Aim: protect sender & receiver privacy and the privacy of exchanged messages
- Combine operations of a mix & a proxy in “router”
- Use multiple routers in a network
routers run by different people

2

Copyright © Scott Bradner & Ben Gaucherin 2016

Onion Routing



- Create paths from sender to destination through multiple routers using “routing onion”
- Sender picks random path through set of known routers
- Knows public keys for routers
- Creates layered set of routing instructions
- Encrypts each layer using public key of a router
- Routers decrypt layer to get next routing instruction

3

Copyright © Scott Bradner & Ben Gaucherin 2016

Onion Routing, contd.

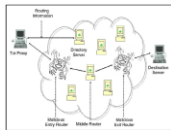


- Data sent along path
 - Equal length packets to make pattern analysis harder
 - Data protected by layers of envelopes
 - Data can be encrypted e2e
- Sender can include a “reply onion” to tell receiver how to send data back to sender

4

Copyright © Scott Bradner & Ben Gaucherin 2016

Onion Routing, contd.



- Compromised router can only find out next hop address, not sender or receiver addresses
 - Except for entry or exit nodes
 - Can get sender or receiver address but does not know it
- 2nd generation onion routing - Tor

5

Copyright © Scott Bradner & Ben Gaucherin 2016

Tor

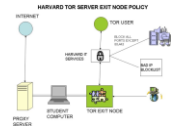


- 2nd generation onion routing system
- Hop-by-hop the sender builds circuit to destination
- Tunnel TCP over circuit once it is established
- Provides “perfect forward secrecy”
 - Disclosure of a key does not impact old communications

6

Copyright © Scott Bradner & Ben Gaucherin 2016

Tor, contd.



- Routers can have different policies
 - Not all routers permit “exit” traffic
 - Routers that permit exit traffic can filter what types of traffic is allowed (i.e., ports)
- Directory servers list known routers and their state

7

Copyright © Scott Bradner & Ben Gaucherin 2016

Tor, contd.



- End-to-end integrity checking
- Original funding from US Navy
- Used by law enforcement to visit suspect sites without disclosing visitor affiliation or identity
- Client uses a proxy to access the Tor network

8

Copyright © Scott Bradner & Ben Gaucherin 2016

Tor: the big picture

Tor: Big Picture

- Freely available (Open Source), unencumbered.
- Comes with a spec and full documentation:
 - Dresden and Aachen implemented compatible Java Tor clients, researchers use it to study anonymity.
- 1500 active relays, 200000+ active users, >1Gbit/s.
- Official US 501(c)(3) nonprofit. Eight full-time developers (!), dozens more dedicated volunteers.
- Funding from US DoD, Electronic Frontier Foundation, Voice of America, a French NGO, Google, NLnet, Human Rights Watch, ...you?

9

Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

Slide#	credit
2	http://ctijournal.com/what-is-onion-routing/
3 & 4	http://cacm.acm.org/magazines/2015/10/192387-seeking-anonymity-in-an-internet-panopticon/fulltext
5	https://homes.cs.washington.edu/~yoshi/papers/Tor/wpe25-bauer.pdf http://www.pcworld.com/article/2848292/malware-served-through-rogue-tor-exit-node-tied-to-cyberespionage-group.html
6	https://commons.wikimedia.org/wiki/File:Tor-logo-2011-flat.svg
7	https://en.wikipedia.org/wiki/File:Exit_Node.jpg
8	https://en.wikipedia.org/wiki/United_States_Naval_Research_Laboratory
9	http://freehaven.net/~arma/slides-25c3.pdf

Surveillance & surveillance avoidance
Tor operation and issues

CSCI E 45b: The Cyber World – part B

1

Copyright © Scott Bradner & Ben Gaucherin 2016

Tor Circuit Setup: 1

- Proxy establishes session key + circuit w R1

2

Copyright © Scott Bradner & Ben Gaucherin 2016

Tor Circuit Setup: 2

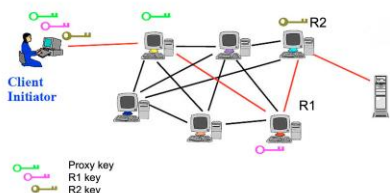
- Proxy tunnels through circuit and extends to R2

3

Copyright © Scott Bradner & Ben Gaucherin 2016

Tor Circuit Setup: 3


- Client applications tunnel TCP through circuit



4 Copyright © Scott Bradner & Ben Gaucherin 2016

Tor: potential issues

- TOR not a magical cloak of invisibility
- Client-and server-side web state not blocked
Cookies & device fingerprints
- Snowden documents show NSA can only crack a small percent of Tor users directly



5 Copyright © Scott Bradner & Ben Gaucherin 2016


Tor: potential issues

- But if user's computer can be compromised then it can be made to give away itself

At least one NSA attack selectively compromised only nodes accessing a honey pot via Tor

Determined by discovering Tor exit nodes using mass monitoring

NSA may also run some Tor nodes



6 Copyright © Scott Bradner & Ben Gaucherin 2016

Tor: Not Just Theory

8,192 routers


Aggregate Network Statistic Summary Graphs / Details	
Total Number of Routers:	8192 100%
Routers in Current Query Result Set:	8192 100%
Total Number of 'Authority' Routers:	8 0.1%
Total Number of 'Bad Directory' Routers:	0 0%
Total Number of 'Bad Exit' Routers:	19 0.23%
Total Number of 'Exit' Routers:	2510 30.64%
Total Number of 'Fast' Routers:	7766 94.8%
Total Number of 'Guard' Routers:	4641 56.65%
Total Number of 'Hibernating' Routers:	0 0%
Total Number of 'Named' Routers:	0 0%
Total Number of 'Stable' Routers:	7387 90.17%
Total Number of 'Running' Routers:	8192 100%
Total Number of 'Valid' Routers:	8192 100%
Total Number of 'V2DIR' Routers:	6742 82.3%
Total Number of 'VSDIR' Routers:	4070 49.68%
Total Number of 'Directory Mirror' Routers:	8 0.1%

as of Jan 2024

https://torstatus.rueckgr.at/
Copyright © Scott Bradner & Ben Gaucher in 2024

7

Tor: Issues




- Used by the bad guys
Spam, child porn, extortion, copyrighted materials, etc.
- FBI knows what Tor is, but investigates Tor routers 'fully and carefully'
Tor operators legally protected (probably) by Communications Decency Act
Exempts network operators from liability for content they do not control
- Not illegal in U.S.
Illegal some places

In August, the Department of Homeland Security pressured a public library in the small town of Lebanon, New Hampshire to shut down a Tor node it was hosting on the popular anonymous browsing network. The unbridled support of dozens of citizens from both Lebanon and the entire country, including off-the-books support from an FBI computer scientist, empowered the town to turn it back on, according to emails obtained by Motherboard.

8

Copyright © Scott Bradner & Ben Gaucher in 2016

Tor: Issues



- Can be very bad PR
Step 0 - the cops think that you are the one doing whatever the person using your Tor exit router is doing through the router

9

Copyright © Scott Bradner & Ben Gaucher in 2016

Tor: Projects

UPDATED

now split off into separate organizations


Our Projects

Tor Browser Tor Browser contains everything you need to safely browse the Internet.	Orbot Tor for Google Android devices.
Tails Live CD/USB operating system preconfigured to use Tor safely.	Nyx Terminal (command line) application for monitoring and configuring Tor.
Relay Search Site providing an overview of the Tor network.	Pluggable Transports Pluggable transports help you circumvent censorship.
Stem Library for writing scripts and applications that interact with Tor.	OONI Global observatory monitoring for network censorship.

<https://www.torproject.org/>

10 Copyright © Scott Bradner & Ben Gaucherin 2021

Tor devices



- **Automatic Tor entry device**
Forwards TCP/IP traffic through the Tor network
- **Anonabox**
Very simple – no user interface
- **InvizBox**
With user interface
- **DIY**
E.g., Raspberry Pi based

11 Copyright © Scott Bradner & Ben Gaucherin 2016

Tor security

Vulnerability could make Tor, the anonymous network, less anonymous

by Ben Bradner | November 1, 2017 10:25 AM EDT | 194 views




Photo: Steve Pappalardo and Ben Gaucherin on their laptop with Tor. Photo: © Steve Pappalardo

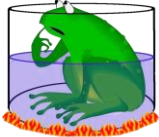
The bad news: MIT and OCRI researchers found a vulnerability in the Tor network. The good news: they also found a fix.

The bad news: MIT and OCRI researchers found a vulnerability in the Tor network. The good news: they also found a fix.

- Vulnerabilities are found in Tor from time to time, they get fixed
- Silk Road was taken down due to operational security issues not Tor vulnerabilities
- But browser vulnerabilities and device fingerprints can compromise users
- Ongoing efforts to create a NG Tor

12 Copyright © Scott Bradner & Ben Gaucherin 2016

Parting thoughts...



Time to worry?

- Surveillance is easy, and common
From governments and businesses alike
General public too often seems complaisant
- Anti-surveillance not easy, and/or user friendly
Sec Ops failures too common

13

Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

Slide#	credit
2-5	Roger Dingledine
5	https://commons.wikimedia.org/wiki/File:National_Security_Agency.svg
6	https://loghythm.com/blog/honeybot-module-announcement/
7	http://torstatus.blutmagie.de
8	https://en.wikipedia.org/wiki/Symbols_of_the_Federal_Bureau_of_Investigation http://motherboard.vice.com/read/this-e-public-comments-saved-a-library-tor-server-from-a-government-shutdown
9	http://www.businessinsider.com/silk-road-alternatives-2013-10
10	https://www.torproject.org/
11	http://arstechnica.com/information-technology/2015/04/review-anon-abox-or-invizbox-which-tor-router-better-anonymizes-online-iff/
12	http://fortune.com/2015/07/29/tor-vulnerability/
13	http://www.bluminated.com/cooking-slowly-where-is-psychotherapeutic-practice-headed-and-do-we-want-to-go-there/

14

Copyright © Scott Bradner & Ben Gaucherin 2016

Surveillance and counter-surveillance
Conclusion

CSCI E 45b: The Cyber World – part B

1 Copyright © Scott Bradner & Ben Gaucherin 2016



Surveillance, wrap up



- Governments, yes - but just governments
- Level of electronic surveillance unimaginable in physical world
Mail, tracking, etc.
- There are some laws relating to surveillance
CALEA, PATRIOT ACT & NSLs, Wiretap Act
- And court cases
Email & GPS tracking

2 Copyright © Scott Bradner & Ben Gaucherin 2016

Surveillance, wrap up, contd.



- Multiple ways that surveillance is preformed
Eavesdropping
Electronic, sound, sound, etc.
Monitoring emissions
Monitoring power
- NSA is representative big player
- Modus operandi successor to Total Information Awareness
Get any and all information

3 Copyright © Scott Bradner & Ben Gaucherin 2016

Surveillance, wrap up, contd.



- Non-government players even bigger
And the government can get their data
- All in the name of advertising (and a “free” Internet)
- Watch out for your boss (or her boss)

4

Copyright © Scott Bradner & Ben Gaucherin 2016

Surveillance, wrap up, contd.



J. Edgar Hoover



- Pervasive surveillance changes society
And puts the population at risk
- Anonymity
Protected for political discussions in U.S.
Used by good guys & bad guys
Outlaw it and the bad guys will use it anyway

5

Copyright © Scott Bradner & Ben Gaucherin 2016

Surveillance, wrap up, contd.

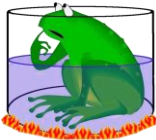


- Some on-line protections exist
- Encryption
- Mixers
- Proxies
- Onion routing
Tor
Works very well, originally government funded – others in government want to do away with it

6

Copyright © Scott Bradner & Ben Gaucherin 2016

Surveillance, wrap up, contd.



- Time to get out of the pot?

7 Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

All drawings and photos by Scott Bradner unless noted

Slide#	credit
2	https://www.quora.com/topic/Communications-Assistance-for-Law-Enforcement-Act-CALEA
	https://commons.wikimedia.org/wiki/File:5es1_of_the_Unit_ed_State_s_Supreme_Court.s
3	http://www.1001modelkits.com/submarines-model-kits/17383-hobby-boss-87004-uss-jimmy-carter-ssn-3-submarine-submarines-6939319270047.html
4	http://adage.com/article/adage/billmore-sun-home-page-ad-turns-back-online-ad-clock/243838/
	http://www.amaticsoft.com/power-spy-software.php
5	http://www.biography.com/people/edgar-hoover-9343398
	http://techland.times.com/2012/05/24/the-new-york-bill-that-would-ban-anonymous-online-speech/
6	https://phpmatters.com/best-drupal-security-modules/
	http://www.poworld.com/article/2848292/malware-served-through-rogue-tor-exit-node-tied-to-cyberespionage-group.html
7	http://www.illuminateded.com/cooking-slowly-where-is-psychotherapeutic-practice-headed-and-do-we-want-to-go-there/

8 Copyright © Scott Bradner & Ben Gaucherin 2016
