



Introduction to Cybersecurity

Prof. Dr. Michael Backes

Director, CISPA – Center for IT Security, Privacy, and Accountability
Chair for IT-security & Cryptography

Organisation

- Course Registration / Course Number (82428)
 - Register **both** in L:admin **and** in HISPOS (links on the course website)
 - **Deadline for registration in L:admin: Monday 27 October 2014, 23:59**
- Lectures: When and where?
 - Thursday 12:00-14:00
 - Building E1 3 – lecture hall 002
- Tutorials:
 - Thursday 14:00-16:00, SR 015 (Oliver Schranz)
 - Friday 12:00-14:00, SR 015 (Kathrin Grosse)
 - Monday 10:00-12:00, SR 014 (Tobias Theobald)
 - Monday 16:00-18:00, SR 107 (Joshua Steffensky)
- Tutorials distributed on **Tuesday, 28 October 2014** (after registration deadline)

CISPA

Foundations of Cybersecurity 2014

1

Organisation

- Tutors' office hour for general questions & advice:
 - Tuesday 12:00-13:00
 - Building E1 3, CIP-R 012
 - Starting Tuesday, 28 October 2014
- Course website:
<http://infsec.cs.uni-saarland.de/teaching/14WS/Cybersecurity>
- Lecture notes / references will be published on website after each lecture
- Mailing list for discussions: cysec14@mail-infsec.cs.uni-saarland.de

CISPA

Foundations of Cybersecurity 2014

2

Organisation

- Teaching assistants

 Malte Skoruppa <i>Part 1:</i> <i>Cryptography</i>	 Sven Bugiel <i>Part 2:</i> <i>System Security</i>
 Erik Derr <i>Part 3:</i> <i>Network Security</i>	 Praveen Manoharan <i>Part 4:</i> <i>Privacy</i>

CISPA Foundations of Cybersecurity 2014 3

Organisation

- Prerequisites:
 - Mathematical / logical understanding
 - Should attend *Programmierung 1* in parallel, or have attended in the past
- Homeworks:
 - Theoretical exercises to be submitted individually
 - Practical projects may be submitted by groups of 2 people
 - Given out at the lecture in written form
 - To be handed in *before the start* of the resp. lecture (typically by email)
 - Email to: cysec14-submissions@mail-infsec.cs.uni-saarland.de
- For some practical projects, you will need CIP pool accounts!
 - Make sure your solutions work on these machines
 - Subscribe for an account by filling out registration form that we hand out

CISPA Foundations of Cybersecurity 2014 4

Organization

- Exam
 - 23rd of February 2015, 9:00-12:00
 - Building E2 2, Günter-Hotz-Hörsaal
- Requirements for passing the course
 - To attend exam, must achieve
 - 50% in theoretical exercises **and**
 - 50% in practical projects
 - To pass the course, must achieve **50%** in exam
- Grading:
 - 60% from exam, 20% from theoretical exercises, 20% from practical projects
- 10 best students will receive offer for research assistant at my chair.

CISPA Foundations of Cybersecurity 2014 5

Why Cyber attacks?

CISPA

Foundations of Cybersecurity 2014

6

Hackers prior to 2003

- Profile:
 - Male
 - Between 14 and 34 years of age
 - Computer addicted
 - No permanent girlfriend



No commercial Interest

Source: Raimund Genes

CISPA

Foundations of Cybersecurity 2014

7

Hackers after 2003 - Commercialization

- Option 1:** bug bounty programs (many)
- Google Vulnerability Reward Program: up to 20K \$
 - For Chrome exploits even up to 50K \$
 - Microsoft Bounty Program: up to 100K \$
 - For Browser exploits up to 100K \$ and for novel browser defenses up to 50K \$
 - Mozilla Bug Bounty program: 500\$ - 3000\$
 - Pwn2Own competition: 15K \$
 - Zero Day Initiative, Verisign iDefense: 2K – 25K \$
 - ZDI even has a 'rewards program' similar to a 'frequent flyer program'

CISPA

Foundations of Cybersecurity 2014

8

Hackers after 2003 - Commercialization

Option 2: Black/Grey Market

- What did a Mozilla zero-day exploit in 2007 buy you?
 - \$500: A Playstation 4
- What did an Adobe Reader zero-day exploit in 2012 buy you?
 - \$5,000 - \$30,000: Extreme gaming PC
- What did an iOS zero-day exploit in 2012 buy you?
 - \$100,000 - \$250,000: 2014 Lamborghini Gallardo



CISPA

Foundations of Cybersecurity 2014

9

Hackers after 2003 - Commercialization

Option 2: Black/Grey market

Zero-Day Prices Over Time

Service	Price	Year
"Some exploits"	\$200,000-\$250,000	2007
"Weaponized exploit"	\$20,000-\$30,000	2007
A "real good" exploit	\$100,000	2007
Microsoft Excel	> \$1,200	2007
Mozilla	\$500	2007
Vista exploit	\$50,000	2007
WMF exploit	\$4,000	2007
ZDI (Defense Purchases)	\$2,000-\$10,000	2007
Adobe Reader	\$5,000-\$30,000	2012
Android	\$30,000-\$60,000	2012
Chrome or Internet Explorer	\$80,000-\$200,000	2012
Firefox or Safari	\$60,000-\$150,000	2012
Flash or Java Browser Plug-ins	\$40,000-\$100,000	2012
iOS	\$100,000-\$250,000	2012
Mac OSX	\$20,000-\$50,000	2012
Microsoft Word	\$50,000-\$100,000	2012
Windows	\$60,000-\$120,000	2012

Source: Rand Corp., National Security Research Division. Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar

CISPA

Foundations of Cybersecurity 2014

10

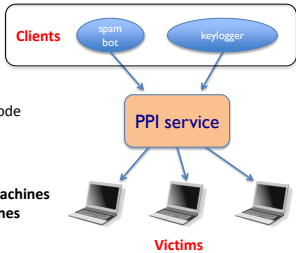
Marketplace for Owned Machines

Pay-per-install (PPI) services

PPI operation:

1. Own victim's machine
2. Download and install client's code
3. Charge client

Cost: US - 100-180\$ / 1000 machines
Asia - 7-8\$ / 1000 machines



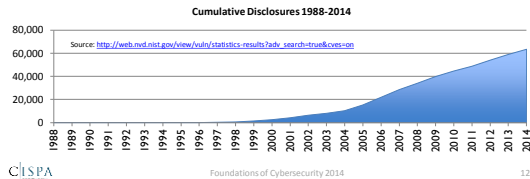
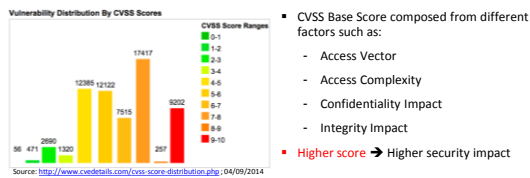
Source: Caballero et al. (www.icir.org/vern/papers/ppi-ussec11.pdf)

CISPA

Foundations of Cybersecurity 2014

11

Tracking vulnerability disclosures



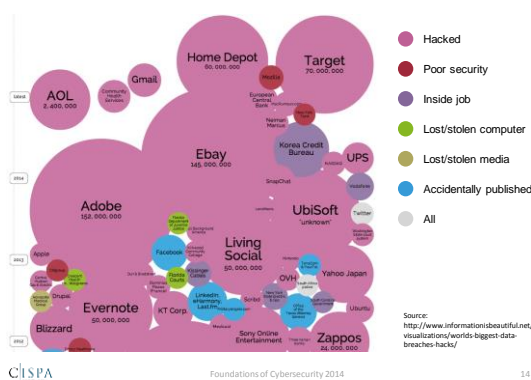
CVSS Score Distribution For Top 30 Products By Total Number Of "Distinct" Vulnerabilities

Product Name	Vendor Name/Number of Total Vulnerabilities	# Of Vulnerabilities	Weighted Average
1 Linux Kernel	Linux 2,000	0-1 1 2 3 4 5 6 7 8 9 10	5.40
2 Firefox	Mozilla 2,000	0-1 1 2 3 4 5 6 7 8 9 10	7.75
3 Windows	Microsoft 1,500	0-1 1 2 3 4 5 6 7 8 9 10	7.90
4 Mac OS X	Apple 1,000	0-1 1 2 3 4 5 6 7 8 9 10	6.60
5 Windows XP	Microsoft 1,000	0-1 1 2 3 4 5 6 7 8 9 10	7.90
6 Mac OS X Server	Apple 1,000	0-1 1 2 3 4 5 6 7 8 9 10	6.60
7 Thunderbird	Mozilla 1,000	0-1 1 2 3 4 5 6 7 8 9 10	8.10
8 Joomla	Open Source 1,000	0-1 1 2 3 4 5 6 7 8 9 10	7.80
9 Mac OS X Server	Apple 1,000	0-1 1 2 3 4 5 6 7 8 9 10	6.70
10 Joomla	Open Source 1,000	0-1 1 2 3 4 5 6 7 8 9 10	6.60
11 Joomla	Open Source 1,000	0-1 1 2 3 4 5 6 7 8 9 10	7.60
12 Windows 2000	Microsoft 1,000	0-1 1 2 3 4 5 6 7 8 9 10	7.60
13 Windows Vista	Microsoft 1,000	0-1 1 2 3 4 5 6 7 8 9 10	8.20
14 Windows Server 2008	Microsoft 1,000	0-1 1 2 3 4 5 6 7 8 9 10	8.10
15 Joomla	Open Source 1,000	0-1 1 2 3 4 5 6 7 8 9 10	7.80
16 Windows 2003 Server	Microsoft 1,000	0-1 1 2 3 4 5 6 7 8 9 10	8.00
17 Joomla	Open Source 1,000	0-1 1 2 3 4 5 6 7 8 9 10	7.80
18 Joomla	Open Source 1,000	0-1 1 2 3 4 5 6 7 8 9 10	7.40
19 Joomla	Open Source 1,000	0-1 1 2 3 4 5 6 7 8 9 10	6.70
20 Joomla	Open Source 1,000	0-1 1 2 3 4 5 6 7 8 9 10	8.20
21 Joomla	Open Source 1,000	0-1 1 2 3 4 5 6 7 8 9 10	8.20
22 Joomla	Open Source 1,000	0-1 1 2 3 4 5 6 7 8 9 10	7.20
23 Joomla	Open Source 1,000	0-1 1 2 3 4 5 6 7 8 9 10	8.00
24 Joomla	Open Source 1,000	0-1 1 2 3 4 5 6 7 8 9 10	7.80
25 Joomla	Open Source 1,000	0-1 1 2 3 4 5 6 7 8 9 10	7.20
26 Joomla	Open Source 1,000	0-1 1 2 3 4 5 6 7 8 9 10	7.20
27 Joomla	Open Source 1,000	0-1 1 2 3 4 5 6 7 8 9 10	7.20
28 Joomla	Open Source 1,000	0-1 1 2 3 4 5 6 7 8 9 10	7.20
29 Joomla	Open Source 1,000	0-1 1 2 3 4 5 6 7 8 9 10	7.20
30 Joomla	Open Source 1,000	0-1 1 2 3 4 5 6 7 8 9 10	7.20

Source: <http://www.cvedetails.com/top-50-product-cvsscore-distribution.php>

CISPA Foundations of Cybersecurity 2014 13

World's biggest data breaches



What is Cybersecurity?

What needs to be secured?

CISPA

Foundations of Cybersecurity 2014

15

Attacking the software – slot machines

- Developer of the software modifies the code
- If a sequence of 10, 5, 25, 10, 5,... cent coins is inserted, the machine gives out the jackpot.



CISPA

Foundations of Cybersecurity 2014

16

- He was caught because he was greedy.

Attacking the software – horse races

- Developer of the software modifies the code
- Allows to place a bet after the race is over.



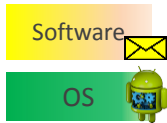
CISPA

Foundations of Cybersecurity 2014

17

- He was caught because he was greedy.

What is Cybersecurity?



CISPA

Foundations of Cybersecurity 2014

19

Hacking Computer via USB

- Virus makes USB key's firmware impersonate a keyboard.



- Stuxnet uses USB keys to attack computers that are not online. Targeting uranium enrichment fabrics in Iran.
 - Goal: Destroy parts of the fabric

CISPA

Foundations of Cybersecurity 2014

20

New era of mobile phone attacks

- **Baseband attacks:** Ralf-Philipp Weinmann discovered that hackers can infiltrate your phone through the airwaves themselves, completely bypassing your operating system and antivirus software to hack directly into the radio processor.
- **USB attacks:** A hidden device packed inside a telephone charger or docking station is casually mining your phone for personal data, stealing all your saved passwords and bathroom mirror self-portraits, and probably slipping you some nasty malware for good measure.



<https://www.usenix.org/conference/woot12/workshop-program/presentation/weinmann>



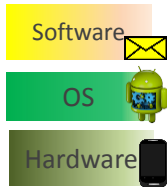
<http://i1227.photobucket.com/albums/ee430/kalista1/malicious-usb-charger.jpg>

CISPA

Foundations of Cybersecurity 2014

21

What is Cybersecurity?



CISPA

Foundations of Cybersecurity 2014

22

Mifare Classic and Crypto

- Used a microscope to see which hardware is inside the card
- Analyzed 10,000 blocks on the chip
- 70 different types
- Reconstructed random number generation
 - Had only 16-bit keys $2^{16} = 65.536$
- Use case of such cards were (!) students' IDs



CISPA

Foundations of Cybersecurity 2014

23

What is Cybersecurity?

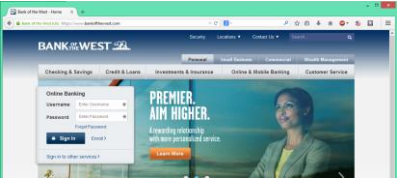


CISPA

Foundations of Cybersecurity 2014

24

Phishing



Looks normal...

...but is not!

CISPA Foundations of Cybersecurity 2014 25

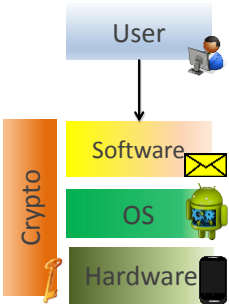
Social Engineering



- Sometimes you just need to ask nicely

CISPA Foundations of Cybersecurity 2014 26

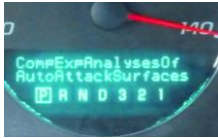
What is Cybersecurity?



CISPA Foundations of Cybersecurity 2014 27

Could Hackers Take Your Car for a Ride?

- **Attacks requiring vehicle access:** Attacks that would control many of the car's systems including the engine, the brakes, and the lights. Attackers could also use specially crafted CDs or Windows Media Audio files that include a Trojan horse to gain control of various automotive systems.
- **Remote attacks:** Attacking weakness in the baseband GPRS cellular and SMS infrastructures used in remote-vehicular assistance services and in Internet-enabled security systems.
- **Recent example(?):** Chinese internet security company Qihoo has announced that it's found ways to remotely control aspects of the Tesla Model S, even while the car is in motion.



<https://www.youtube.com/watch?v=yT8trnSDQk>



http://upload.wikimedia.org/wikipedia/commons/2/23/Tesla_Model_S_digital_panels.jpg

CISPA

Foundations of Cybersecurity 2014

28

Stealing cars with a laptop

- Security technology created to protect luxury vehicles may now make it easier for tech-savvy thieves to drive away with them.
- High-tech criminals made international headlines when they used a laptop and transmitter to open the locks and start the ignition of an armor-plated BMW X5 belonging to soccer player David Beckham, the second X5 stolen from him using this technology within six months.

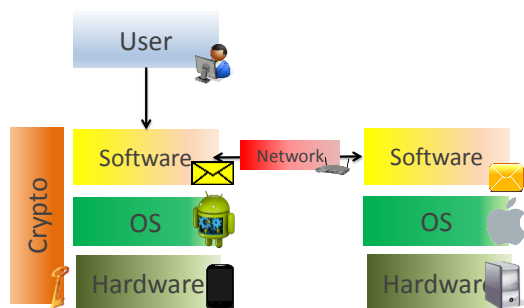


CISPA

Foundations of Cybersecurity 2014

29

What is Cybersecurity?



CISPA

Foundations of Cybersecurity 2014

31

That's all?

Even more attack vectors

CISPA

Foundations of Cybersecurity 2014

32

When 'Smart Homes' Get Hacked: I Haunted A Complete Stranger's House Via The Internet

- The flawed security of home automation system HomeMatic was revealed by hackers Sathya and Malli at the 30th Chaos Communication Congress (30C3). HomeMatic enables users to **unlock doors, control the heater or receive alerts from a motion detector**. Performing three live hacks within an hour Sathya and Malli showed how they were able to gain **unauthorized access and take over control of each of those functions**.
- Hacking the grid took on new meaning at the DefCon hacker conference when two independent security researchers demonstrated two tools they designed to hack home and business automation and security systems that **operate through power lines**.



<http://electronic-lifestyle.com/wp-content/uploads/2013/09/home-automation.jpg>



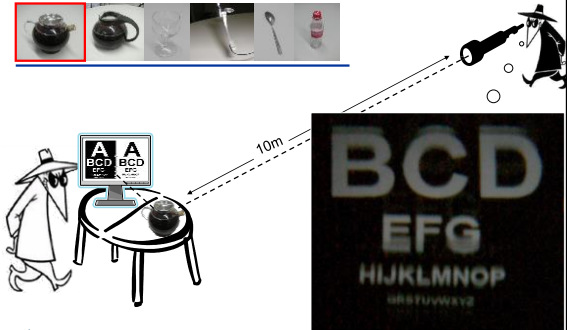
http://www.wired.com/images_blog/htreatlevel/2013/08/x10-jammer.png

CISPA

Foundations of Cybersecurity 2014

33

Exploiting reflections to spy on secrets

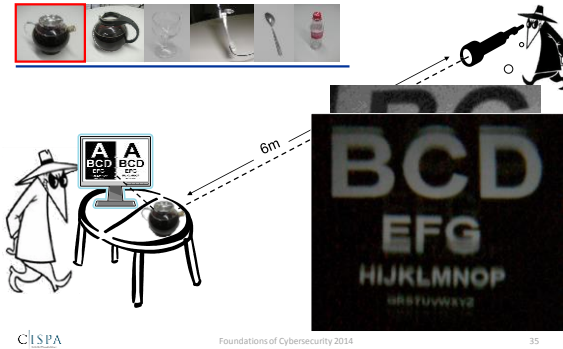


CISPA

Foundations of Cybersecurity 2014

34

Exploiting reflections to spy on secrets

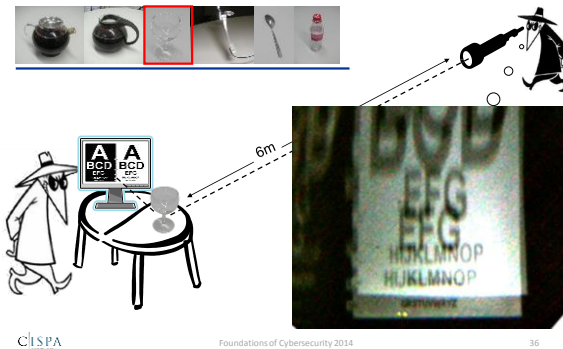


CISPA

Foundations of Cybersecurity 2014

35

Exploiting reflections to spy on secrets

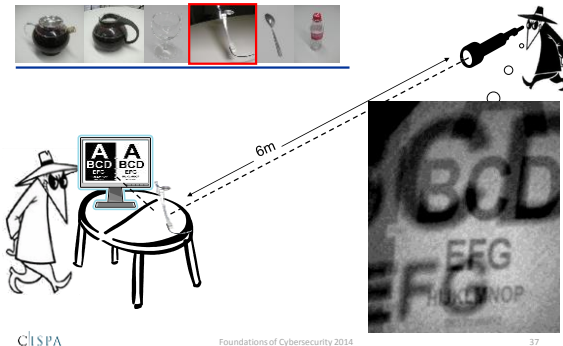


CISPA

Foundations of Cybersecurity 2014

36

Exploiting reflections to spy on secrets

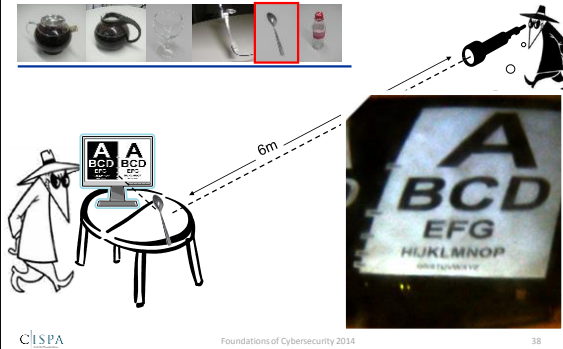


CISPA

Foundations of Cybersecurity 2014

37

Exploiting reflections to spy on secrets

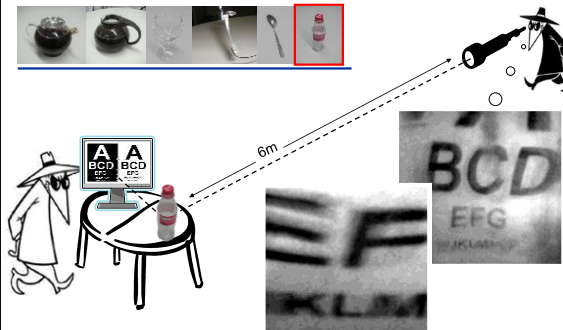


CISPA

Foundations of Cybersecurity 2014

38

Exploiting reflections to spy on secrets



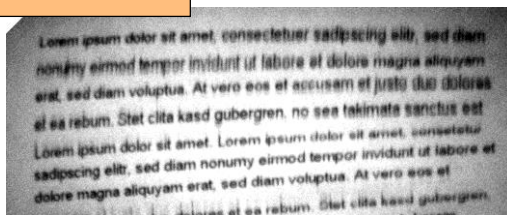
CISPA

Foundations of Cybersecurity 2014

39

Spying on an actual Word document

- Distance approx. 7 meters
- 12pt font (readable)



CISPA

Foundations of Cybersecurity 2014

40

Acoustic side-channel attacks

Man with a secret

Dot-matrix printer

Merciless attacker

CISPA

Foundations of Cybersecurity 2014

41

Why would you care?

- Are dot-matrix printers still used
... for anything confidential ...
... that I would care for?
- Commissioned large survey in Germany
 - Dot-matrix printers used by more than 60% of doctors:
 - medical prescriptions,
 - receipts,
 - patients transfers...
 - Used by more than 30% of banks:
 - account statements,
 - PIN numbers...
- Printing prescription of narcotic substances **only allowed on dot-matrix printer by law**
(in Germany, Switzerland, Austria, ...)

CISPA

Foundations of Cybersecurity 2014

42

Why is this all difficult to avoid?

CISPA

Foundations of Cybersecurity 2014

43

In general: Why is security so difficult?

- **Functionality**
 - If user does **(some expected input)**
Then system does **(some expected action)**
- **Security**
 - If a user or outsider does **(some unexpected thing)**
Then system does **not do (any really bad action)**
- **Why is security difficult?**
 - What are **all possible unexpected things?**
 - How do we know that **all** of them are protected?
 - At what level of system abstraction?

CISPA

Foundations of Cybersecurity 2014

44

Security Objectives

- What do we want to achieve in computer security?
 - **Confidentiality:** Ensuring that information is not accessed by unauthorized persons (e.g., access control or encryption)
 - **Integrity:** Ensuring that information is not altered by unauthorized persons in a way that is not detectable by authorized users (e.g., access control or checksums)
 - **Availability:** Ensuring timely and reliable access to and use of information and preventing unauthorized withholding of information.
 - **Authenticity:** Ensuring that users are the persons they claim to be.
 - Different other objectives:
 - Non-repudiation, accountability, privacy, anonymity, unlinkability,...
 - Topic of other chapters in this course and of other courses

CISPA

Foundations of Cybersecurity 2014

45

Where to realize computer security?

- Security can be realized at different levels
 - **Physical world**
 - Example threats: Theft or lost devices
 - Example security measures: Guards, fences, doors
 - **Hardware**
 - Example threats: Probing or dismantling hardware components, hardware debuggers
 - Example security measures: Tamper resistant devices, tamper reactive devices, tamper evident devices
 - **Software**
 - Example threats: Software exploits, malicious drivers/firmware
 - Example security measures: Various system hardening techniques, cryptographic means
 - **Network**
 - Example threats: Intercepting/manipulating network traffic
 - Example security measures: Cryptographic means and protocols, physical isolating networks

CISPA

Foundations of Cybersecurity 2014

46

Realizing Security in Practice

- Design can be good
- But implementation can be insecure
 - If implementation allows more actions than design, then attack can succeed as a result of implementation error
 - Why? Implementations embedded into larger contexts, with additional capabilities and constraints.

CISPA

Foundations of Cybersecurity 2014

47

If you remember one thing from this part...

A vulnerability that is “too complicated
for anyone to ever find” *will* be found!

I hope you remember more than one thing.

CISPA

Foundations of Cybersecurity 2014

48



**Introduction to Cybersecurity
Cryptography (Part 1)**

Prof. Dr. Michael Backes

Director, CISPA – Center for IT Security, Privacy, and Accountability
Chair for IT-security & Cryptography

Assumptions on System Security

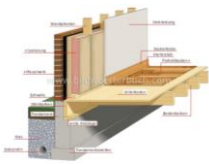
- Important to remember from the start:
 - Avoid “security by obscurity” !
 - Worst-case scenario and realistic in nowadays systems
 - Corruption, threats of physical safety, etc.
- Goal:
 - System should be secure even if source code is public
 - Only secret: short key (*Kerckhoff’s principle*)
- Proprietary algorithms = bad algorithms

CISPA

Foundations of Cybersecurity 2014

50

Difference to the Cryptography lecture



- Overview
- Conceptual
- The way people use crypto
- Systematical constructions
- Proofs in detail
- The way people invent crypto

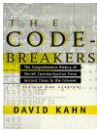
CISPA

Foundations of Cybersecurity 2014

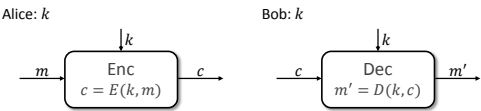
51

On (Historic) Ciphers

- History: David Kahn “The Codebreakers”



Ciphers:



Symmetric encryption: Both Alice and Bob use the same key k

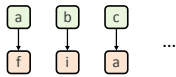
CISPA

Foundations of Cybersecurity 2014

52

Ancient Ciphers: Substitution Cipher

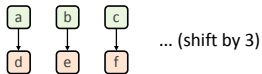
- Oldest cipher in the world, used in the bible, etc.
- Key k is:



- Encryption of plaintext $m = \text{"cbaa"}$ gives ciphertext
 $c = E(k, m) = \text{"aiff"}$
- #Keys = $26! \approx 2^{86}$

Ancient Ciphers: Caesar's Cipher

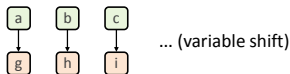
- Used by Caesar in Ancient Rome, 70 B.C.
- Key is fixed table (i.e., actually no cipher):



- Encryption and decryption as for the substitution cipher

Ancient Ciphers: Shift Cipher

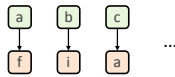
- Generalization of Caesar's cipher



- E.g., ROT-13 is an example of a shift cipher historically used:
 - In newsgroups (1980s) and forums, to make text unreadable
 - Actually used in *Netscape Navigator* as part of an insecure scheme to store passwords (1999)
- Encryption and decryption as for the substitution cipher
- #Keys = 26

Ancient Ciphers: Substitution Cipher

- Oldest cipher in the world, used in the bible, etc.
- Key k is:



- Encryption of plaintext $m = \text{"cbaa"}$ gives ciphertext
 $c = E(k, m) = \text{"aiff"}$

- #Keys = $26! \approx 2^{86}$

- Easy to break:

- Letter frequency analysis: "e" 12.7%, "t" 9.1%, "a" 8.1%
- Frequency of pairs of letters: "th", "he", "in"
- → Ciphertext-only attack!

CISPA

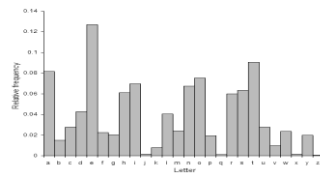
Foundations of Cybersecurity 2014

56

Letter Frequencies

- Letter frequencies in average English text. Most common:

- e, t, a, o, i, n
- s, h, r, d, l, u
- ...



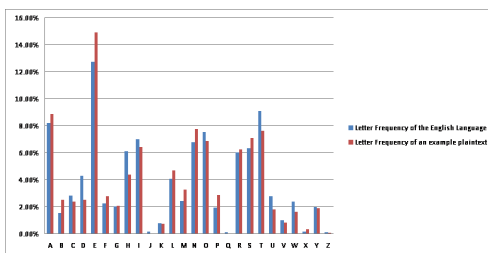
- Common bigrams are:
 - th, he, in, en, nt, re, er, an
- Common trigrams
 - the, and, tha, ent, ing, ion

CISPA

Foundations of Cybersecurity 2014

57

Sample Text Distribution

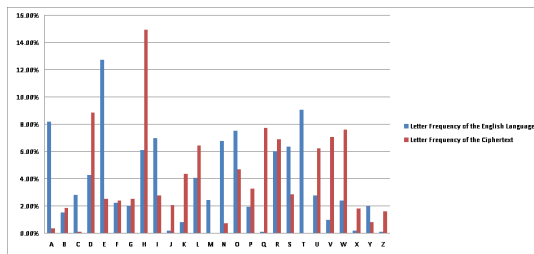


CISPA

Foundations of Cybersecurity 2014

58

Corr. Ciphertext Distribution (shift by 3 - Caesar)



CISPA

Foundations of Cybersecurity 2014

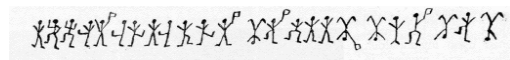
59

Examples of Substitution Ciphers

- Edgar Allan Poe, "The Gold Bug"

53++(305))6*;4826(4+.)4+);806*;4818'60))85;|8*;;+*8183(88)5*!;
 46(,88*96*?;8)*+{(485);5*!2.*+{(4956*2(5*4)8'8*;4069285);)6
 |8|4++;1(+9;48081;8:8+1;48185;4)4851528806*81(+9;48;(88;4(+73
 4;48)4+;161;:188;+?;

- Sir Arthur Conan Doyle's "Adventure of the Dancing Men"



CISPA

Foundations of Cybersecurity 2014

60

Examples of Substitution Ciphers

- Edgar Allan Poe, "The Gold Bug"

A good glass in the bishop's hostel in the devil's seat twenty-one degrees and thirteen minutes northeast and by north main branch seventh limb east side shoot from the left eye of the death's-head a bee line from the tree through the shot fifty feet out.

- Sir Arthur Conan Doyle's "Adventure of the Dancing Men"

ELSIE PREPARE TO MEET THY GOD

CISPA

Foundations of Cybersecurity 2014

61

Cryptanalysis of Substitution Cipher (1)

vxr fezfvtvevtan ytxrs tf nav fryesr

Letter frequencies

- v: 5
- r, t, f: 4
- e: 3
- x, a, n, s, y: 2
- j, z: 1

Bigrams

- xr: 2

Guess

vxr=THE

a b c d e f g h i j k l m n o p q r s t u v w x y z

CISPA

Foundations of Cybersecurity 2014

62

Cryptanalysis of Substitution Cipher (2)

vxr fezfvtvevtan ytxrs tf nav fryesr

THE _T_T_T_ _HE_ _T_E_E_

Letter frequencies

- t, f: 4
- e: 3
- a, n, s, y: 2
- j, z: 1

Bigrams

- Es, sE: 1

Guess

s=R

a b c d e f g h i j k l m n o p q r s t u v w x y z

E T H

CISPA

Foundations of Cybersecurity 2014

63

Cryptanalysis of Substitution Cipher (3)

vxr fezfvtvevtan ytxrs tf nav fryesr

THE _T_T_T_ _HER_ _T_E_RE

Letter frequencies

- t, f: 4
- e: 3
- a, n, y: 2
- j, z: 1

Bigrams

Guess

na=NO

a b c d e f g h i j k l m n o p q r s t u v w x y z

E R T H

CISPA

Foundations of Cybersecurity 2014

64

Cryptanalysis of Substitution Cipher (4)

vxr fezfvtvevtan ytxrs tf nav fryesr

THE _ _ _ T _ T _ ON _ _ HER _ _ NOT _ E _ RE

Letter frequencies

-
- t, f: 4
- e: 3
- y: 2
- j, z: 1

Bigrams



Guess

tf=IS

a b c d e f g h i j k l m n o p q r s t u v w x y z
O N E R T H

CISPA

Foundations of Cybersecurity 2014

65

Cryptanalysis of Substitution Cipher (5)

vxr fezfvtvevtan ytxrs tf nav fryesr

THE S _ STIT _ TION _ I _ HER IS NOT SE _ RE

Letter frequencies

-
- e: 3
- y: 2
- j, z: 1

Bigrams



Guess

guess

a b c d e f g h i j k l m n o p q r s t u v w x y z
O S N E R I T H

CISPA

Foundations of Cybersecurity 2014

66

Cryptanalysis of Substitution Cipher (6)

vxr fezfvtvevtan ytxrs tf nav fryesr

THE SUBSTITUTION CIPHER IS NOT SECURE

Letter frequencies

Bigrams



Guess

a b c d e f g h i j k l m n o p q r s t u v w x y z
O U S P N E R I T H C B

CISPA

Foundations of Cybersecurity 2014

67

Ancient Ciphers: Vigenère Cipher

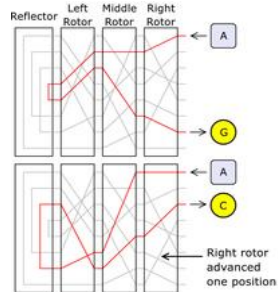
- By Vigenère, 1523 – 1570
- Key is randomly chosen string of certain length n .
- Encryption (by means of example)

m = THISISBLACKART
K = CRYPTOCRYPTO

c = VYGHBGDCYRDOTK (add mod 26)

- #Keys = $26^n \approx 2^{4.7n}$
- Easy to break, again frequency analysis

The Enigma machine



Old Ciphers: Rotor Machines

- Roughly 1800 – 1940s.
- Key is initial position of the rotor
- Encryption and decryption by rotations, presumably hard to invert without knowing starting position
- With nowadays knowledge easy to break even by ciphertext-only attacks.

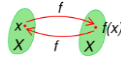
Enigma – some Problems and Weaknesses

- Reflector weakens Enigma: no difference between en- and decryption

- Problem 1: encryption becomes involuntary, i.e.

- if $K \rightarrow T$, then $T \rightarrow K$

- Problem 2: no letter is encrypted to itself
(electricity can't go same way back)



→ Heavy reduction of encryption alphabet

- Violation of Kerckhoff's principle:

- Security of Enigma depended on wiring of rotors

- Wiring was part of algorithm, not part of key

- Wiring never changed from 1920s until 1945
