

CE4062/CZ4062

Computer Security

Lecture 1: Introduction

Tianwei Zhang

Teaching Staff Members

Lecturers:

- ▶ Asst. Prof. Zhang Tianwei (1st half): tianwei.zhang@ntu.edu.sg
- ▶ Dr. Tay Kian Boon (2nd half, course coordinator): kianboon.tay@ntu.edu.sg

Teaching Assistants


- ▶ Wang Hanqin: hanqin001@e.ntu.edu.sg
- ▶ Zhou Jianan: jianan004@e.ntu.edu.sg

Attack Motivation – Financial Profit

Steal personal data and sell them to the black market

17 Feb 2021 09:00PM
(Updated: 18 Feb 2021 11:26AM)

Nearly 130,000 Singtel customers' personal information, including NRIC details, **stolen in data breach**



A Singtel logo is seen on its building in Singapore, Aug 11, 2016. (File photo: AFP/Roslan Rahman)

SINGAPORE: Personal information of nearly 130,000 Singtel customers was stolen after a recent data breach of a third-party file-sharing system, the local telco said on Wednesday (Feb 17).

Singtel has completed initial investigations into the breach and established which files on the **Accellion file transfer appliance were accessed illegally**, the company said in a news release.

SINGAPORE
Singapore health system hit by 'most serious breach of personal data' in cyberattack; PM Lee's data targeted

By Kevin Kwang
@KevinKwangCNA

20 Jul 2018 05:29PM
(Updated: 18 Oct 2018 11:17AM)

Singapore
Singapore health system hit by **'most serious breach of personal data'** in cyberattack; PM Lee's data targeted

A total of 1.5 million SingHealth patients' non-medical personal data were stolen, while 160,000 of those had their dispensed medicines' records taken too, according to MCI and MOH.

Passwords and usernames of staff from MOH, MOE and other agencies stolen and put up for sale by hackers



Attack Motivation – Financial Profit

Steal credit card information or bank accounts

- ▶ Malware targeting different devices: ATM, POS machine, website...

News

Target credit card data was sent to a server in Russia

The data was quietly moved around on Target's network before it was sent to a US server, then to Russia

By Jeremy Kirk

January 16, 2014 08:49 PM ET 23 Comments

in Share 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000

IDG News Service - The stolen credit card numbers of millions of Target shoppers took an international trip -- to Russia.

A peek inside the malicious software that infected Target's POS (point-of-sale) terminals is revealing more detail about the methods of the attackers as security researchers investigate one of the most devastating data breaches in history.

Findings from two security companies show the attackers breached Target's network and stayed undetected for more than two weeks.

Over two weeks the malware collected 11GB of data from Target's POS terminals, said Aviv Raff, CTO of the security company [Seculert](#), in an interview via instant message on Thursday. Seculert analyzed a sample of the malware, which is circulating among security researchers.

The data was first quietly moved to another server on Target's network, according to a [writeup](#) on Seculert's blog, It was then transmitted in chunks to a U.S.-based server that the attackers had hijacked. Raff said.

In its Jan. 14 analysis, iSight wrote that the "Trojan.POSRAM" malware collected unencrypted payment card information just after it was swiped at Target and while it sat in a POS terminal's memory. The type of malware it used is known as a RAM scraper.

The code of "Trojan.POSRAM" bears a strong resemblance to "BlackPOS," another type of POS malware, iSight wrote. BlackPOS was being used by cyberattackers [as far back as](#) March 2013.

Although Trojan.POSRAM and BlackPOS are similar, the Target malware contains a new attack method that evades forensic detection and conceals data transfers, making it hard to detect,

Attack Motivation – Financial Profit

Ransomware

- ▶ Inject into the computer, encrypt the data and request for ransom



WannaCry ransomware

Attack Motivation – Politics

Government actors

Private activism

Stuxnet 'hit' Iran nuclear plans

22 November 2010



Behind the 'Flame' malware spying on Mideast computers (FAQ)

With possible ties to malware targeting Iran, the Flame spying software is seen as the latest cyber espionage attempt from a nation state.



Elinor Mills

June 4, 2012 6:28 a.m. PT

8 min read



WikiLeaks supporters disrupt Visa and MasterCard sites in 'Operation Payback'

MasterCard and Visa attacked after restricting dealings with WikiLeaks - and hackers say Twitter is next



Supporters of Julian Assange in London. WikiLeaks supporters Anonymous have launched a campaign of online attacks against perceived enemies. Photograph: Peter Macdiarmid/Getty Images

Emerging Security Issues with New Technologies and Situations

Zoom's Security and Privacy Issues

News



Zoom boss apologises for security issues and promises fixes

🕒 2 April 2020 [Source: https://www.bbc.com/news/technology-52133349](https://www.bbc.com/news/technology-52133349)



'Zoom is malware': why experts worry about the video conferencing platform

The company has seen a 535% rise in daily traffic in the past month, but security researchers say the app is a 'privacy disaster'

Thu 2 Apr 2020 15:23 BST

[Source: https://www.theguardian.com/technology/2020/apr/02/zoom-technology-security-coronavirus-video-conferencing](https://www.theguardian.com/technology/2020/apr/02/zoom-technology-security-coronavirus-video-conferencing)



Zoom boosts encryption to quell safety concerns as users top 300 million

22 Apr 2020 09:55PM

[Source: https://www.channelnewsasia.com/news/business/zoom-boosts-encryption-to-quell-safety-concerns-as-users-top-300-million-12667956](https://www.channelnewsasia.com/news/business/zoom-boosts-encryption-to-quell-safety-concerns-as-users-top-300-million-12667956)



Zoom strikes a deal with NY AG office, closing the inquiry into its security problems

PUBLISHED THU, MAY 7 2020 3:54 PM EDT

[Source: https://www.cnbc.com/2020/05/07/zoom-strikes-a-deal-with-ny-ag-office-closing-security-inquiry.html](https://www.cnbc.com/2020/05/07/zoom-strikes-a-deal-with-ny-ag-office-closing-security-inquiry.html)

- Zoom's **randomly-generated meeting ID No. could be predicted** (and even brute-forceable), allowing bad actors to intrude, disrupt and eavesdrop on meetings. The company subsequently replaced meeting IDs with a "cryptographically strong" one and made passwords a default for users to join a meeting.
- Security flaw in the app could let websites hijack Mac cameras.** The company subsequently patched its software and uninstalled a local web server that created the vulnerability.
- The app **sent data about a user's time zone and city, as well as details about the user's device to Facebook**, even if the user did not have a Facebook account.
- The company tightened their privacy policy after concerns surfaced about user's personal information being used to target ads.
- Zoom allegedly leaked user information because of an issue with how the app grouped contacts.
- Zoom allegedly **misled users to believe video meetings were secured with end-to-end encryption** instead of transport encryption.

Emerging Security Issues with New Technologies and Situations

Covid-19 pandemic meets new security challenges

News

Watch out for fake govt websites and links by scammers taking advantage of COVID-19 situation

Published on 28 Apr 2020

Source: <https://www.gov.sg/article/watch-out-for-fake-govt-websites-and-links-by-scammers-taking-advantage-of-covid-19-situation>

SingCERT warns of fake COVID-19 contact tracing apps containing malware

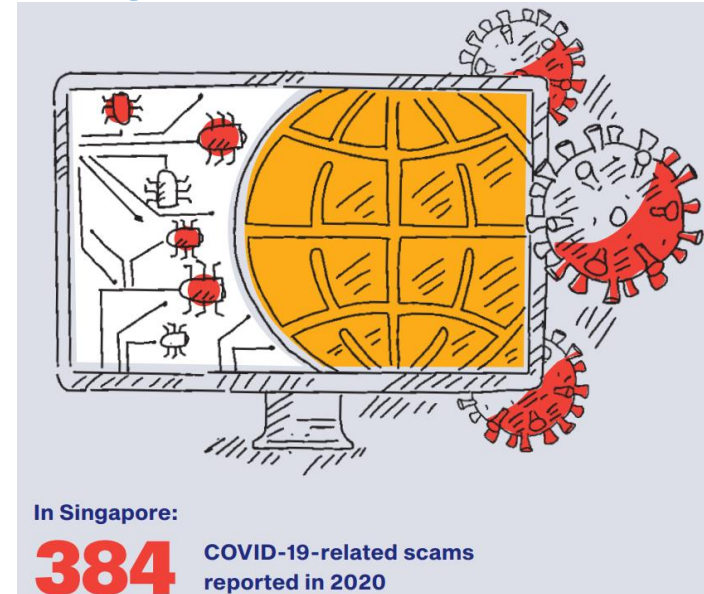
Singapore 12 Jun 2020 03:59PM

Source: <https://www.channelnewsasia.com/news/singapore/covid-19-singcert-fake-contact-tracing-apps-download-privacy-12829624>

Cybercriminals are exploiting fears of the pandemic to steal personal information

PUBLISHED WED, APR 15 2020 1:18 AM EDT

Source: <https://www.cnn.com/2020/04/15/coronavirus-cybercriminals-are-targeting-people-through-phishing-scams.html>



- Uptick in number of cases involving cybercriminals attempting to **capitalise on COVID-19 to steal personal information and credentials** which will allow them to gain access to networks and/or make financial gains.

- Some malware strains deployed* include known credential-stealing malware such as AZORult, Cerberus, Lokibot and TrickBot.

- There are **fake contact tracing apps** that are embedded with malware that can be used to conduct malicious activities, such as monitoring users' activities on their devices or stealing personal data.

- These threats have proliferated across many sectors, including **healthcare, manufacturing, pharmaceutical and transportation**.

Source: [Capitalising on COVID-19 Pandemic](#), CSA (published 1 April 2020)

Singapore Cyber Landscape 2021

Overview of Cyber Threats in 2021



NUMBER OF CASES HANDLED BY SINGCERT:

2021: **7,342**

2020: **9,080**

2019: **8,491**

PHISHING

55,000

phishing URLs¹ with a Singapore-link were detected, an increase from 47,000 in 2020

1. URLs — Uniform Resource Locators; colloquially termed web addresses.

COMMONLY SPOOFED SECTOR



1ST > SOCIAL NETWORKING



2ND > FINANCIAL



3RD > ONLINE/CLOUD SERVICE

WHATSAPP, FACEBOOK, LLOYDS, CHASE BANK AND MICROSOFT WERE COMMONLY SPOOFED BRANDS



ONLINE CHEATING

2021: **18,068**

2020: **12,242**

2019: **7,580**



COMPUTER MISUSE ACT

2021: **3,731**

2020: **3,482**

2019: **1,701**



CYBER EXTORTION

2021: **420**

2020: **245**

2019: **68**

CYBERCRIME IN SINGAPORE

Cybercrime cases accounted for

48%

of overall crime in 2021

WEBSITE DEFAACEMENTS

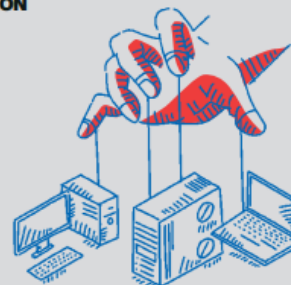
Singapore-linked website defacements were detected, a slight decrease from 495 in 2020

RANSOMWARE

137

cases of ransomware were reported to SingCERT in 2021, a 54% increase from 89 cases in 2020

COMMAND AND CONTROL (C&C) SERVERS AND BOTNET DRONES



3,300

unique C&C servers were observed in Singapore, more than triple the 1,026 unique C&C servers in 2020

4,800

botnet drones (compromised computers infected with malicious programs) with Singapore Internet Protocol (IP) addresses were observed daily on average, a decrease from 2020's daily average of 6,600

Singapore Cyber Landscape 2021

Significant Cyber Incidents in 2021

GLOBAL INCIDENTS

Jan 2021

Use of zero-day vulnerabilities in Accellion's FTA* software for data breaches and extortions.

*File Transfer Appliance

Jan - Mar 2021

Mass exploitation of zero-day vulnerabilities in Microsoft's Exchange Server.

Feb 2021

Attempted poisoning of Florida's water supply via cyber intrusion.

May 2021

Colonial Pipeline hit by *Darkside* ransomware.

May 2021

JBS Foods attacked by *REvil* ransomware.

Jul 2021

REvil ransomware delivered via Kaseya's VSA* software.
*Virtual System Administrator

Jul 2021

Exposé on NSO Group's *Pegasus* spyware.

Jul 2021

Cyber-attack on Iranian train systems.

Aug 2021

Alleged targeting of telcos in Southeast Asia by APT groups.

Nov 2021

Cyber-attack on Iranian gas stations.

Nov 2021

Emotet makes a comeback.

Dec 2021

Exploitation of Log4j vulnerabilities.

LOCAL INCIDENTS

Jan 2021

Singtel data breach via Accellion's FTA.

Mar - Aug 2021

Multiple companies suffer ransomware attacks and data extortion by ALTDOS.

Jul 2021

StarHub data breach involving third-party data dump site.

Sep 2021

Exploitation of SMS one-time-password verification channel for credit card fraud.

Aug 2021

Ransomware attack on Eye & Retina Surgeons.

Aug 2021

Unauthorised access of MyRepublic's mobile customers' data.

Nov 2021

Cyber-attack with data theft on Swire Pacific Offshore.

Dec 2021

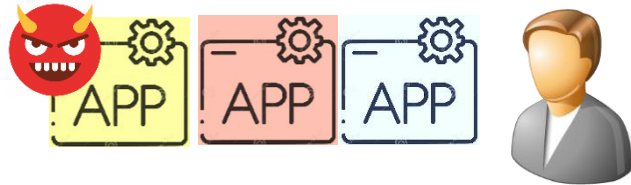
High-profile phishing scams targeting OCBC customers.

Computer System Security

Provide a protected environment for data and their processing

**Standalone computer
single user
monoprogram**

Physical security



**Standalone computer
single user
multiprogram**

Physical security

Process protection



**Standalone computer
multiple user**

Physical security

Process protection

Data protection

User authentication



Networked computer

Physical security

Process protection

Data protection

User authentication

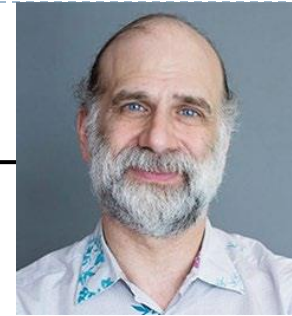
**Communication
protection**

Why is Security so Hard



“Security engineering is about building systems to remain dependable in the face of malice, error, or mischance.”

-- Rose Anderson



“Security involves making sure things work, not in the presence of random faults, but in the face of an intelligent and malicious adversary trying to ensure that things fail in the worst possible way at the worst possible time ... again and again. It is truly programming Satan’s computer.”

-- Bruce Schneier

System Security Failures

Secure information systems may be broken because:

- ▶ Cryptographic algorithms are broken
- ▶ Security features are not designed correctly
- ▶ Security features are not used correctly
- ▶ Security components are not implemented correctly
- ▶ Security components are not configured properly
- ▶ Security is not managed properly
- ▶ Threat environment may change and assumption invalid

Learning Outcome

Understand vulnerabilities associated with computer systems, and how they can be mitigated.

Understand security mechanisms in modern computer systems, its role and its importance.

Understand techniques for implementing security policies

Administrative Matters

Each week we have (full-time):

- ▶ A two-hour lecture (8:30 – 10:30am Friday, **physical at LT2A**)
- ▶ A one-hour tutorial (10:30 – 11:30am Monday).
 - ▶ First tutorial is in Week 3 (Public holiday – will release the video recording for e-learning)
 - ▶ Week 4 – Week 7: **physical at LT1**

Each week we have (part-time):

- ▶ A three-hour lecture & tutorial (starting at 7pm Monday, **physical at TR+3**)

Course materials will be made available through NTULearn

Assessment

2 Quizzes (35% each)

- ▶ Quiz 1: lecture slot in week 7
 - ▶ Full-time: 8:30 – 9:30am 24 February
 - ▶ Part-time: 7:00 – 8:00pm 20 February
- ▶ Quiz 2: lecture slot in week 13
 - ▶ Full-time: 8:30 – 9:30am 14 April
 - ▶ Part-time: 7:00 – 8:00pm 10 April
- ▶ Those who are validly absent must take make up quiz. Failure to do so will get 0 marks.

Assessment

Project (30% each)

- ▶ Groups of 4 students
- ▶ Each group does 2 case studies about real-world computer security incidents.
- ▶ Set in Week 14 for a 15-minute onsite presentation (10 minutes presentation + 5 minutes Q&A)
- ▶ All members must do the presentation & understand BOTH projects.
- ▶ Sign up for the groups (deadline: 11:59pm 31 January). Make sure no duplicated names. Note there are two tabs for full-time and part-time separately. After the deadline, we will allocate the groups for the students not in the list.

<https://docs.google.com/spreadsheets/d/16DsXxz55xMpFN36BAemUMViuRV8ldV6GrR-DQuJIK1s/edit?usp=sharing>

Assessment

Project judge criterion

- ▶ Real-world computer security incidents, better to have significant impacts.
- ▶ The cases should be related to the content discussed in this course, but do not directly use the examples introduced in the lecture.
- ▶ Technical depth: describe the technical details about the mechanism of the incidents. It is recommended to perform code analysis for the vulnerabilities. Having demos will be a plus.
- ▶ Clear presentation. Able to correctly answer the questions.

Schedule (Full-time)

Week	Tutorial	Lecture	Instructor
I		Introduction	Zhang Tianwei
2		Software Security I	
3	Software Security I	Software Security II	
4	Software Security II	Software Security III	
5	Software Security III	OS Security I	
6	OS Security I	OS Security II	
7	OS Security II	Quiz I	
8-12	Passwords & Authentication Mobile security Computer Security Case studies Introduction to Cryptography		Tay Kian Boon
13		Quiz 2	
14	Final Presentation		

Schedule (Part-time)

Week	Lecture & Tutorial	Instructor
1	Introduction	Zhang Tianwei
2	Software Security I	
3	Software Security II	
4	Software Security III	
5	OS Security I	
6	OS Security II	
7	Quiz I	
8-12	Passwords & Authentication Mobile security Computer Security Case studies Introduction to Cryptography	Tay Kian Boon
13	Quiz 2	
14	Project presentation	

References

No required textbooks. If you want extra reading:

- ▶ D. Gollmann, **Computer Security** (3rd ed.), John Wiley & Sons, 2011.
- ▶ M. Bishop, **Computer Security: Art and Science**, Addison-Wesley, 2003.
- ▶ R. Anderson, **Security Engineering**, 2008.
- ▶ Erickson, **Hacking: the art of exploitation**, 2nd Edition, 2008.

Basics of Computer Security

- ▶ **Trust and Trusted Computing Base**
- ▶ **Threat Model**
- ▶ **Security Properties**
- ▶ **Security Strategies**
- ▶ **Design Principles of Computer Security**

Trust

The degree to which an entity is expected to behave:

- ▶ What the entity is expected to do: anti-malware can detect malicious programs; system can prevent illegal account login, etc.
- ▶ What the entity is expected not to do: the website will not expose your private data to third parties; an application will not inject virus into your system.

Security cannot be established in a computer system if no entities are trusted.

It is important to make clear what should be trusted. Otherwise, the designed security solutions may fail in practice.

Trusted Computing Base (TCB)

A set of system components (e.g., software, OS, firmware, hardware) that need to be trusted to ensure the security of the computer system

Components outside of the TCB can be malicious and misbehave.

When we design a security solution, we need to

- ▶ Assume all the components inside the TCB are secure with valid justifications.
- ▶ Prevent any damages from any components outside of the TCB.

Size of TCB

- ▶ A system with a smaller TCB is more trustworthy (we do not need to make too many assumptions, which may be violated)
- ▶ Designing a secure system with a smaller TCB is more challenging (we need to consider more malicious entities)

Threat Model

Describe the adversaries in consideration

- ▶ What is trusted and what is not trusted.
- ▶ For the untrusted entities, what resources, capabilities and knowledge they have; what actions they can perform.
- ▶ What security properties the system aim to achieve.

An example: phishing email – a malicious email with malware as the attachment

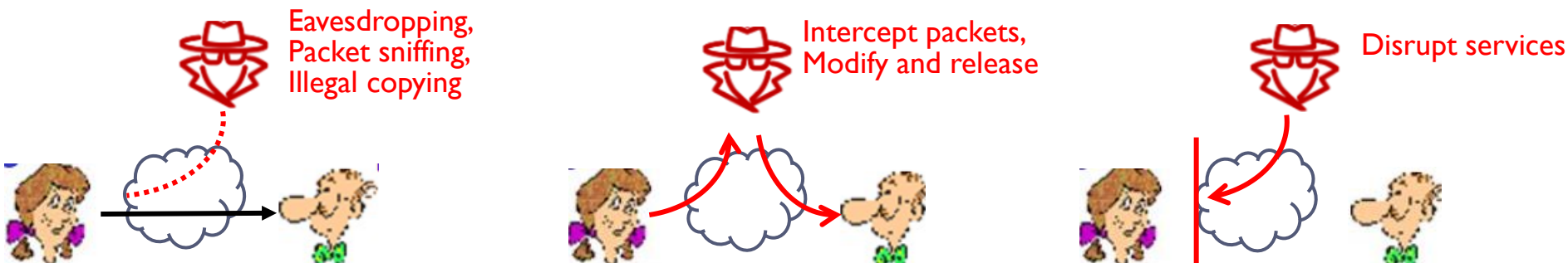
- ▶ What is trusted: hardware and OS
- ▶ What is not trusted: the email attachment.
- ▶ Adversarial capabilities: running malicious code in your computer.
- ▶ Security properties: protect the computer system such that the malware cannot steal the sensitive data, or tamper with other processes.

Security Properties

The security goals that we aim to achieve for the system.

Common security properties (CIA model)

- ▶ Confidentiality (C): prevent unauthorized **disclosure** of information. Sensitive information should not be leaked to unauthorized parties
- ▶ Integrity (I): prevent unauthorized **modification** of information. Critical system state and code cannot be altered by malicious parties
- ▶ Availability (A): prevent unauthorized **withholding** of information or resources. The resources should be always available for authorized users



Security Properties

Other properties

- ▶ Accountability: actions of an entity can be traced and identified
- ▶ Non-repudiation: unforgeable evidence that specific actions occur
- ▶ Authenticity: ensure the communicated entity is the correct entity.

Security Strategies

Prevention

- ▶ Take measures that prevent your system from being damaged

Detection

- ▶ Take measures so that you can detect when, how, and by whom your system has been damaged.

Reaction

- ▶ Take measures so that you can recover your system or to recover from a damage to your system.

Design Principles of Computer Security

Principle of least privilege

- ▶ An entity should be given the minimal permissions to complete its task.
- ▶ Give the privilege when needed, and revoke the privilege after use
- ▶ If granting unnecessary permissions, a malicious entity could abuse those permissions to perform the attack.

Principle of separation of privilege

- ▶ Separation of duty: for multiple entities working together, it is better to distribute privileges to different entities.
- ▶ A single malicious party cannot get all the privileges to perform the attack.

Defense in depth

- ▶ Multiple types of defenses should be layered together
- ▶ Increase the difficulty of attacking the entire system.