Intelligent Security Systems
Chapter 5
Hackers vs. normal users
Who is our enemy and how to differentiate them from us?

Abstract

The module starts with discussing how hacker's demography and their culture have been changing over the years. Then it proceeds with presenting hacking attacks, techniques and tools as well as anti-hacking protection mechanisms. In the second part it moves to the ordinary user's profiles and authentication. Here we show how to employ data science and statistical approaches to find out and analyze user's characteristics and their influence on the security level of their computer practice. The chapter presents the computer device security evaluation procedures. It discusses how to conduct analysis, observations, results, and recommendations for users to improve their overall security practices and the security of their devices. Also, it examines the hacking web fingerprinting attacks against the privacy protection TOR technology that utilizes machine learning as well as possible protection mechanisms. Examples and use cases are included.

Learning Outcomes

Upon completion of this lesson, students will be able to:

- classify hackers and their activities and use a professional terminology in the field for their description and identification
- understand and apply anti-hacking protection principles and to employ artificial intelligence and machine learning techniques to differentiate legitimate users from attackers with authentication and other mechanisms
- analyze and plan privacy protection tools, systems and procedures

Contents

Required Reading

- L.Reznik **Intelligent Security Systems:** How artificial intelligence, machine learning, and data science work for and against computer security. IEEE-Wiley, 2022, **Chapter 5**

Part 1:
Hacker's activities and protection against

Intelligent Security Systems
Chapter 5
Hackers vs. normal users

Hackers activities and protection against: Content

Modules	Slides
1. Definition or Who is a hacker?	
2. History and philosophy of hackers	
3. Hacker's classification	
4. Hacker's motives	
5. Typical hacker activities.	
6. Hacking tools	
7. Anti-hacking protection	
8. Use design case: Recurrent neural networks for colluded applications attack detection in Android OS devices	

Who are hackers?

Every security breach highlights something the victim didn't do or a mistake that wound up being very costly, such as reusing passwords or not running firewall software.

Some of the attacks can be quite sophisticated, using zero-day vulnerabilities.

Or sometimes they are or just plain devious, relying on phishing scams.

Many people tend to think of hackers as geniuses as they are often one step ahead of the good guys.

In general, hackers are "very calculating and successful," so there aren't a lot of "dumb hacks" out there, according to Marc Maiffret, CTO of eEYE Digital Security, told eWEEK.

Who is spying on you?

- In July 2014 Russian crime ring CyberVog made cybersecurity history by amassing the largest known collection of stolen Internet credentials, including 1.2 billion user name and password combinations and more than 500 million email addresses.
- In 2013 Target theft netted credit and debit card information from 40 million customers and personal information, including email addresses and phone numbers, from up to an additional 70 million customers.

Who is spying on you?

- In 2013 Ed Snowden copied and leaked classified information from NSA without prior authorization. His disclosures revealed numerous global surveillance programs, many run by the NSA and the Five Eyes Intelligence Alliance with the cooperation of telecommunication companies and European governments.
- Who else? Your insurance company? Your boss?

Kevin Mitnick

Kevin David Mitnick (born on August 6, 1963) is a computer security consultant, author, and hacker. In the late 20th century, he was convicted of various computer- and communications-related crimes. At the time of his arrest, he was the most-wanted computer criminal in the United States.

- **Confirmed criminal acts**
- Using the Los Angeles bus transfer system to get free rides
- Evading the FBI
- Hacking into DEC system(s) to view VMS source code (DEC reportedly spent $160,000 in cleanup costs)
- Gaining full administrator privileges to an IBM minicomputer at the Computer Learning Center in Los Angeles in order to win a bet
- Hacking Motorola, NEC, Nokia, Sun Microsystems and Fujitsu Siemens systems

https://tophackers.wordpress.com/1-kevin-mitnick/

Kevin Mitnick

Alleged criminal acts

- Stole computer manuals from a Pacific Bell telephone switching center in Los Angeles
- Read the e-mail of computer security officials at MCI Communications and Digital
- Wiretapped the California DMV
- Made free cell phone calls
- Hacked Santa Cruz Operation, Pacific Bell, FBI, Pentagon, Novell, California Department of Motor Vehicles, University of Southern California and Los Angeles Unified School District systems.
- Wiretapped NSA agents, according to John Markoff. This was originally denied by Kevin Mitnick but later mentioned by Mitnick while listing his crimes as a juvenile in an interview with Stephen Colbert on an August 18, 2011 episode of *The Colbert Report*.

Source: Wikipedia

FBI Most wanted cyber criminals Oct. 2021

- On May 28, 2021, a federal grand jury in the United States District Court for the Southern District of California returned an indictment against four People's Republic of China (PRC) citizens for their alleged roles in a long running campaign of computer network operations targeting trade secrets, intellectual property, and other high value information from companies, universities, research institutes, and governmental entities in the United States and abroad, as well as multiple foreign governments. The indictment alleges that Zhu Yunmin, Wu Shurong, Ding Xiaoyang, and Cheng Qingmin targeted the following sectors: aerospace/aviation, biomedical, defense industrial base, healthcare, manufacturing, maritime, research institutes, transportation (rail and shipping), and virus research from 2012 to 2018, on behalf of the PRC Ministry of State Security. Additionally, the indictment alleges the use of front companies by the PRC Ministry of State Security to conduct cyber espionage.

Source: FBI.gov

Source: FBI.gov

FBI Most wanted cyber criminals Oct. 2021

- Mujtaba Raza and Mohsin Raza are wanted for allegedly operating a fraudulent online business based in Karachi, Pakistan. Since at least 2011, the business known as SecondEye Solution (SecondEye), aka Forwarderz, allegedly sold digital images of false identity documents including passports, driver's licenses, bank statements, and national identity cards associated with more than 200 countries and territories. SecondEye marketed these fake documents for use verifying online accounts, which allowed SecondEye customers to defraud payment processing companies, e-commerce businesses, social media, and social networking platforms. On January 28, 2020, a federal arrest warrant was issued for Mujtaba Raza in the United States District Court, District of New Jersey, Newark, New Jersey, after he was charged with Conspiracy to Produce and Transfer False Documents, Transfer of False Documents, False Use of Passports, and Aggravated Identity Theft.

Source: FBI.gov

FBI Most wanted cyber criminals Oct. 2021

- Park Jin Hyok is allegedly a state-sponsored North Korean computer programmer who is part of an alleged criminal conspiracy responsible for some of the costliest computer intrusions in history. These intrusions caused damage to computer systems, and stole currency and virtual currency from, numerous victims.
- Park was alleged to be a participant in a wide-ranging criminal conspiracy undertaken by a group of hackers of the North Korean government's Reconnaissance General Bureau (RGB). The conspiracy comprised North Korean hacking groups that some private cybersecurity researchers have labeled the "Lazarus Group" and Advanced Persistent Threat 38 (APT38). On December 8, 2020, a federal arrest warrant was issued for Park in the United States District Court, Central District of California, after he was charged with one count of conspiracy to commit wire fraud and bank fraud, and one count of conspiracy to commit computer fraud (computer intrusions). A federal arrest warrant was previously issued for Park on June 8, 2018, after he was charged with one count of conspiracy to commit wire fraud and one count of conspiracy to commit computer-related fraud (computer intrusion) in a federal criminal complaint.

Source: FBI.gov

FBI Most wanted cyber criminals Oct. 2021

- On October 15, 2020, a federal grand jury sitting in the Western District of Pennsylvania returned an indictment against six Russian military intelligence officers for their alleged roles in targeting and compromising computer systems worldwide, including those relating to critical infrastructure in Ukraine, a political campaign in France, and the country of Georgia; international victims of the "NotPetya" malware attacks (including critical infrastructure providers); and international victims associated with the 2018 Winter Olympic Games and investigations of nerve agent attacks that have been publicly attributed to the Russian government. The indictment charges the defendants, Sergey Vladimirovich Detistov, Yuriy Sergeyevich Andrienko, Pavel Valeryevich Frolov, Anatoliy Sergeyevich Kovalev, Artem Valeryevich Ochichenko, and Petr Nikolayevich Pliskin, with a computer hacking conspiracy intended to deploy destructive malware and take other disruptive actions, for the strategic benefit of Russia, through unauthorized access to victims' computers. The indictment also charges these defendants with false registration of a domain name, conspiracy to commit wire fraud, wire fraud, intentional damage to protected computers, aggravated identity theft, and aidin

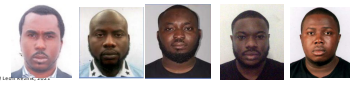
Source: FBI.gov

FBI Most wanted cyber criminals Oct. 2021

- Uzuh and his co-conspirators, Alex Afolabi Ogunshakin, Felix Osilama Okpoh, Abiola Ayorinde Kayode, and Nnamdi Orson Benson, allegedly sent spoofed emails to thousands of businesses in the United States requesting fraudulent wire transfers. Uzuh allegedly worked with money launderers, romance scammers, and others involved in BEC schemes to launder the proceeds of their crimes through a complex network of witting and unwitting people in the United States and abroad. On October 18, 2016, Uzuh was indicted in the United States District Court, District of Nebraska, Omaha, Nebraska, on charges of Wire Fraud and Conspiracy to Commit Wire Fraud. On October 19, 2016, a federal warrant was issued for his arrest.

Source: FBI.gov

Source: FBI.gov



watch video

How The FBI Caught The Most Wanted Hacker In History

Time: 10:07

https://www.youtube.com/watch?v=IgTysqEsevk

Top 10 Most Wanted Hackers in the World

Time: 4:39

https://www.youtube.com/watch?v=nkJUXnG7MtU

Answer the questions:

How would you classify those hackers? What are their typical characteristics? What would be the right strategy and detect and protect against them?

Who are hackers? Definition, please?

Hacker is defined as

(1) one that hacks;

(2) a person who is inexperienced or unskilled at a particular activity;

(3) an expert at programming and solving problems with a computer, and

(4) a person who illegally gains access to and sometimes tampers with information in a computer system.

Source: Meriam-Webster on-line dictionary – accessed at https://www.merriam-webster.com/dictionary/hacker on Dec. 16, 2020

Who are hackers? History

The roots of diversity among hackers could be traced in part to two historical documents in the hacker subculture:

the Hacker Ethic [Levy 1984] and

the Hacker Manifesto [Mentor 1986]

The hacker ethic originated at the Massachusetts Institute of Technology in the 1950s-1960s. The term "hacker" had long been used there to describe college pranks that MIT students would regularly devise, and was used more generally to describe a project undertaken or a product built to fulfill some constructive goal but also out of pleasure for mere involvement

Source: Wikipedia

Refs: S. Levy, Hackers: Heroes of the Computer Revolution. Dell, New York, 1984.

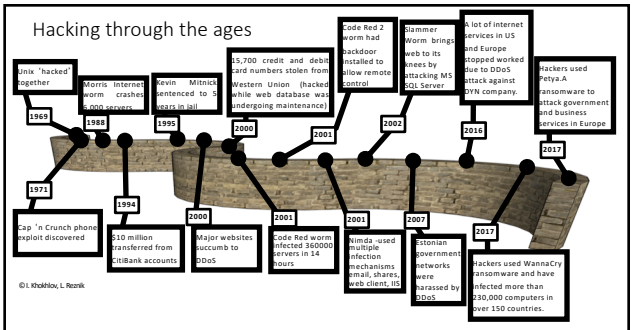
The Mentor, The conscience of a hacker, 1986, http://www.wbglinks.net/pages/reads/misc/hackersmanifesto.

Who are hackers? History

- ***The Conscience of a Hacker*** (also known as ***The Hacker Manifesto***) is a small essay written January 8, 1986 by a computer security hacker who went by the handle of The Mentor (born Loyd Blankenship), who belonged to the 2nd generation of hacker group Legion of Doom.
- It was written after the author's arrest, and first published in the underground hacker ezine *Phrack* and can be found on many websites, as well as on T-shirts and in films.
- Considered a cornerstone of hacker culture,the *Manifesto* asserts that there is a point to hacking that supersedes selfish desires to exploit or harm other people, and that technology should be used to expand our horizons and try to keep the world free.

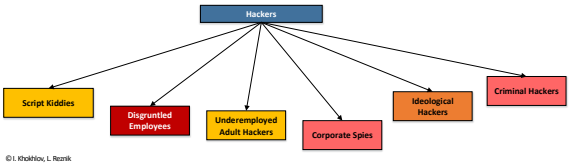
Source: Wikipedia

Hacking through the ages



© I. Khokhlov, L. Reznik

Hacker Classification Attempt



© I. Khokhlov, L. Reznik

Hacker Classification Attempt

- **Script kiddies** - mostly kids/students
  Use tools created by black hats.
  Motivation:
  - To get free stuff
  - Impress their peers
  - Not get caught
- **Underemployed Adult Hackers** - former Script Kiddies
  Motivation:
  - Can' t get employment in the field
  - Want recognition in hacker community
  - Big in eastern European countries
- **Ideological Hackers**
  - hack as a mechanism to promote some political or ideological purpose
  - Usually coincide with political events

Hacker Classification Attempt

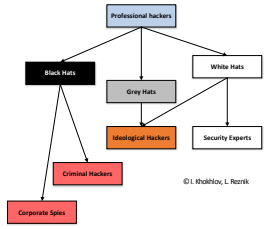
- **Criminal Hackers**
  - Real criminals, are in it for whatever they can get no matter who it hurts
- **Corporate Spies**
  - Are relatively rare
- **Disgruntled Employees**
  - Most dangerous to an enterprise as they are "insiders"
  - Since many companies subcontract their network services a disgruntled vendor could be very dangerous to the host enterprise

Professional Hackers

Professional hackers:

- **Black Hats** – the "bad guys", malicious hackers who cause harm or break laws as part of their hacking exploits.
- **White Hats** – usually a professional security experts/consultants, who offer hacking/penetration testing as part of their services. Hackers who don't break the law, commit any offense or engage in any malicious activity as part of their hacking.
- **Grey Hats** - hackers whose actions are not malicious but whose hacking methods may break legal laws or ethical standards. Hackers who may at one stage have broken the law, but who have since come across to the more ethical white side.

Source: http://searchsecurity.techtarget.com/answer/What-is-red-and-white-hat-hacking



Legal Recourse

- Average armed robber will get $2500-$7500 and risk being shot or killed; 50-60% will get caught , convicted and spent an average of 5 years of hard time
- Average computer criminal will net $50K-$500K with a risk of being fired or going to jail; only 10% are caught, of those only 15% will be turned in to authorities; less than 50% of them will do jail time
- Prosecution
  - Many institutions fail to prosecute for fear of advertising
    - Many banks absorb the losses fearing that they would lose more if their customers found out and took their business elsewhere
      - Fix the vulnerability and continue on with business as usual

Top intrusion motivations and justifications

- I'm doing you a favor pointing out your vulnerabilities
- I'm making a political statement
- Because I can
- Because I'm paid to do it

Top intrusion motivations and justifications

- *Profit :* sought to exploit any and all weaknesses that they found in computers and computer networks for their own profit. The hackers would attempt to create as much damage as possible and make the maximum amount of money they could while doing so.
- *Protest* Hackers for revealing illegal and immoral activities of corrupt governments, scandals and toxic activities of corporations and identities and details of individuals involved in nefarious accounts.
- *Enjoyment and/or challenge* for testing their capabilities and intellect. Some hackers do so for the sheer vicarious pleasure they derive from such activities.
- *Betterment* for finding faults and weaknesses, but instead of exploiting them, bring them to the attention of the organization or entity whose systems possess these faults.

What are Black Hat, White Hat, and Grey Hat Hackers?
Time: 2:17
https://www.youtube.com/watch?v=E6S3-XGrZAE
What Are The 7 Types Of Hackers [Explain a comprehensive list of all the types of hackers]
Time: 7:32
https://www.youtube.com/watch?v=CHb9iSKV_dI

Answer the questions:

Do you think the difference between various hackers is important in real life? Why yes or no? Or do you think they change their designation a way too often?

Hacker's Activities

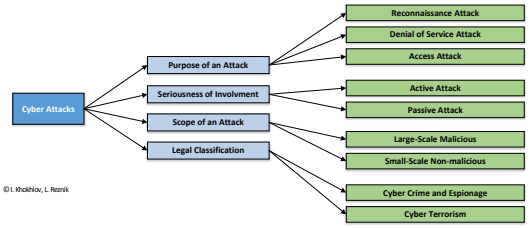
Typical activities of a hacker include, but are not limited to:

compromising network security,

- breaking into and disabling application software currently running on the network/machine (some hackers attempt to install their own malicious programs) and
- seeking to use a machine or network they broke into, to further their uses.

Hackers often use malware to corrupt the victim system in order to gain control and then either complete their mission (extract and then disseminate information, attempt to blackmail their victim after obtaining information, etc), or they use the viruses for different purposes.

Classification of Cyber Attacks/Hacking activities



Purpose of Attack

- **Reconnaissance attack** is an attempt to gather sensitive information about network services and system
  - **Packet Sniffers**
  - **Ping Sweep**
  - **Port Scan**
  - **Queries Regarding Internet information**
- **Denial of Service Attack** is a network attack devised to slow down or crash a system by flooding it with useless traffic.
  - **Ping of Death**
  - **Teardrop Attack**
- **Access Attacks** is when an attacker may try to uncover exploits and vulnerabilities in FTP, Web Services and Network Authentication in order to get access to a system's network.
  - **Password Attack**
  - **Trust Exploitation Attack**
  - **Man in the middle**

Seriousness of Involvement

- An **active attack** allows the attacker to block the communication channel between participants on a network or permits him to send data to all the parties at once.
- **Passive attack** is when an intruder with unauthorized network access actively eavesdrops a communication between two participants.

Attack Scope

- **Malicious Large-Scale Attack:**

Malicious attack is an offensive attempt or an intent to inflict harm, such attacks aim at creating chaos and disrupting services.

- **Non-Malicious Small-Scale Attack:**

An unintentional attack or an accidental damage due to a human operational error that might cause a system crash, deletion of data, is a non-malicious attack.

Legal Classification

- **Cyber Crime and Espionage:**

Any crime that encompasses a network or a computer can be deemed as **cyber crime**. The practice of gathering secrets without the consent of the information holder using a Computer System or Network is termed as **cyber espionage**.

- **Cyber Terrorism:**

Instances of terrorism in the cyberspace domain are classified under **cyber terrorism**.

Recent Hacker's Activities
-**Kaseya 'Ransomware Apocalypse'**

The malicious cyberattack on global IT provider Kaseya just ahead of the July 4 weekend in 2021 has certainly screwed up a lot of stuff for a lot of people, affecting potentially as many as 1,500 businesses all over the world, bringing down local governments, shuttering a popular Swedish chain of supermarkets.

The attack, which infected a popular Kaseya software product called VSA, was used to spread malware to dozens of the company's customers—many of which were managed service providers, or MSPs, firms that help small businesses and government agencies with outsourced IT tasks.

The cybercriminal gang behind the attack, the Russian-speaking group REvil, initially asked for $70 million in return for a "universal decryptor" that would unlock all of the files that the single attack has frozen worldwide. By mid-July, however, the group appeared to have gone underground.

See https://www.youtube.com/watch?v=6E2X35spjwk for more information

Source: https://gizmodo.com/the-biggest-hacks-of-2021-so-far-1847157024

Recent Hacker's Activities
- **SolarWinds Megabreach**

- The hack, which U.S. authorities believe involved Russian (and maybe Chinese) threat actors worming their way into the networks of major federal agencies and American companies via compromised software, helped said hackers gather untold amounts of intelligence on the U.S. government and private sector. While the incident was first publicized in December 2020, subsequent disclosures about the extent of the hack have continued.
- Despite being commonly referred to as "SolarWinds," the hack actually involved a compromise of at least three different software firms, including SolarWinds, Microsoft, and VMWare, according to the Cybersecurity and Infrastructure Security Agency (CISA). A total of 12 federal agencies are confirmed to have been penetrated by the hackers. The hackers also allegedly wormed their way into the networks of major Fortune 500 companies.
- Watch https://www.youtube.com/watch?v=VrLJQjiHZeY for more details

Source: https://gizmodo.com/the-biggest-hacks-of-2021-so-far-1847157024

Recent Hacker's Activities
- The Colonial Pipeline attack

- is likely the most important cyberattacks of the year so far—both for its ability to show the devastating potential of cybercrime and for the robust federal response it inspired.
- In May, hackers affiliated with the ransomware gang DarkSide managed to get inside the network of Colonial Pipeline, one of America's largest oil and gas companies. By temporarily halting the pipeline's operations, the attack not only spurred a short-lived energy crisis throughout the Southeast but also fundamentally shifted how the federal government approaches cyberattacks of this nature. Following the attack, the FBI managed to trace and seize a significant portion of the cryptocurrency ransom payment that Colonial made to the hackers—a somewhat unprecedented development.
- See https://www.youtube.com/watch?v=Z7QkdrkKkVc for more information

Source: https://gizmodo.com/the-biggest-hacks-of-2021-so-far-1847157024

New fields and opportunities for malicious hacking

New digital devices, such as locks, sensors, kitchen appliances, connected to internet, replace mechanical parts and can open up new fields and opportunities for hacking attacks

Images taken at CES 2018 @ I.Khokhlov and L.Reznik

watch video

The SolarWinds Hack And The Future Of Cyber Espionage
https://www.youtube.com/watch?v=jxTxGlE9X5s
Time: 9:26

Answer the questions:
Do you think sybersecurity is over-publicized and, may be even over-politicized? Or on the contrary, more factual information has to be provided to the public?

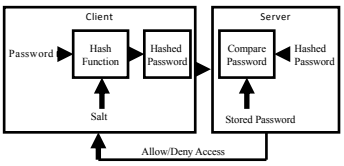
Phases of hacker's attacks

Gaining access

- Front door
  - Password guessing
  - Password/key stealing
- Back doors
  - Often left by original developers as debug and/or diagnostic tools
  - Forgot to remove before release
- Trojan Horses
  - Usually hidden inside of software that we download and install from the net (remember nothing is free)
  - Many install backdoors
- Software vulnerability exploitation
  - Often advertised on the OEMs web site along with security patches
  - Fertile ground for script kiddies looking for something to do

Password Attacks

- Password hashed and stored
  - Salt added to randomize password & stored on system
- Password attacks launched to crack encrypted password



Password Attacks - Process

- Find a valid user ID
- Create a list of possible passwords
- Rank the passwords from high probability to low
- Type in each password
- If the system allows you in – success !
- If not, try again, being careful not to exceed password lockout (the number of times you can guess a wrong password before the system shuts down and won't let you try any more)

Brute Force Attack and Social Engineering

- **Social engineering** is the act of manipulating people into performing actions or divulging confidential information. **One of the most powerful methods of hacking**.
- **Brute Force** is a cryptanalysis technique or other kind of attack method involving an exhaustive procedure that tries all possibilities, one-by-one.

Source: https://www.sans.org/security-resources/glossary-of-terms/

Password Attacks - Types

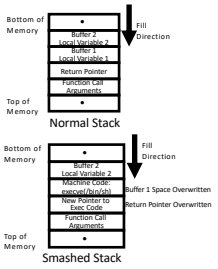
- **Dictionary Attack**
  - Hacker tries all words in dictionary to crack password
  - 70% of the people use dictionary words as passwords
- **Brute Force Attack**
  - Try all permutations of the letters & symbols in the alphabet
- **Hybrid Attack**
  - Words from dictionary and their variations used in attack
- **Social Engineering**
  - People write passwords in different places
  - People disclose passwords naively to others
- **Shoulder Surfing**
  - Hackers slyly watch over peoples shoulders to steal passwords
- **Dumpster Diving**
  - People dump their trash papers in garbage which may contain information to crack passwords

Software vulnerability exploitation

- Buffer overruns/overflow
- HTML / CGI scripts
- Poor design of web applications
  - Javascript hacks
  - PHP/ASP/ColdFusion URL hacks
- Other holes / bugs in software and services
- Tools and scripts used to scan ports for vulnerabilities

Buffer Overflow Attacks

- This attack takes advantage of the way in which information is stored by computer programs
- An attacker tries to store more information on the stack than the size of the buffer



Buffer Overflow Attacks

- Programs which do not have a rigorous memory check in the code are vulnerable to this attack
- Simple weaknesses can be exploited
  - If memory allocated for name is 50 characters, someone can break the system by sending a fictitious name of more than 50 characters
- Can be used for espionage, denial of service or compromising the integrity of the data

Examples:

- NetMeeting Buffer Overflow
- Outlook Buffer Overflow
- AOL Instant Messenger Buffer Overflow
- SQL Server 2000 Extended Stored Procedure Buffer Overflow

Once inside, the hacker can...

- Modify logs
  - To cover their tracks
  - To mess with you
- Steal files
  - Sometimes destroy after stealing
  - A pro would steal and cover their tracks so to be undetected
- Modify files
  - To let you know they were there
  - To cause mischief
- Install back doors
  - So they can get in again
- Attack other systems

Spoofing

Spoofing is when an attacker alters his identity so that someone thinks he is someone else.

Exploits:

- Email, User ID, IP Address, …
- Attacker exploits trust relation between user and networked machines to gain access to machines

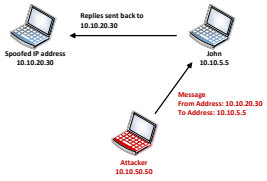
Types of Spoofing:

1. IP Spoofing
2. Email Spoofing
3. Web Spoofing

IP Spoofing – Flying-Blind Attack

Is when an attacker uses IP address of another computer to acquire information or gain access.

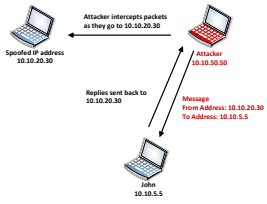
- Attacker changes his own IP address to spoofed address
- Attacker can send messages to a machine masquerading as spoofed machine
- Attacker can not receive messages from that machine



IP Spoofing – Source Routing

Is when an attacker spoofs the address of another machine and inserts itself between the attacked machine and the spoofed machine to intercept replies.

- The path a packet may change can vary over time
- To ensure that he stays in the loop the attacker uses source routing to ensure that the packet passes through certain nodes on the network



Email Spoofing

Is when an attacker sends messages masquerading as someone else.

What can be the repercussions?

Types of Email Spoofing:

- Create an account with similar email address:
  yourprofessor@yahoo.com: A message from this account can perplex the students
- Modify a mail client:
  Attacker can put in any return address he wants to in the mail he sends
- Telnet to port 25:
  Most mail servers use port 25 for SMTP. Attacker logs on to this port and composes a message for the user.

Web Spoofing

Basic attack:

- Attacker registers a web address matching an entity e.g. votetrump.com, geproducts.com, gesucks.com

Man-in-the-Middle Attack:

- Attacker acts as a proxy between the web server and the client
- Attacker has to compromise the router or a node through which the relevant traffic flows

URL Rewriting attack:

- Attacker redirects web traffic to another site that is controlled by the attacker
- Attacker writes his own web site address before the legitimate link

Tracking State attack:

- When a user logs on to a site a persistent authentication is maintained
- This authentication can be stolen for masquerading as the user

Session Hijacking

Session Hijacking is a process of taking over an existing active session

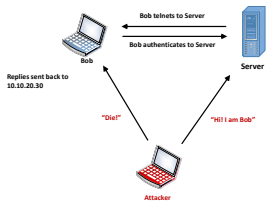
Modus Operandi:

1. User makes a connection to the server by authenticating using his user ID and password.
2. After the users authenticate, they have access to the server as long as the session lasts.
3. Hacker takes the user offline by denial of service
4. Hacker gains access to the user by impersonating the user

Session Hijacking

Attacker can :

- monitor the session
- periodically inject commands into session
- launch passive and active attacks from the session



Session Hijacking – How Does it work?

- Attackers exploit sequence numbers to hijack sessions
- Sequence numbers are 32-bit counters used to:
  - tell receiving machines the correct order of packets
  - Tell sender which packets are received and which are lost
- Receiver and Sender have their own sequence numbers
- When two parties communicate the following are needed:
  - IP addresses
  - Port Numbers
  - Sequence Number
- IP addresses and port numbers are easily available so once the attacker gets the server to accept his guesses sequence number he can hijack the session.

Denial of Service (DoS) Attack

DoS is an attack through which a person can render a system unusable or significantly slow down the system for legitimate users by overloading the system so that no one else can use it.

Types:

- Crashing the system or network
  - Send the victim data or packets which will cause system to crash or reboot.
- Exhausting the resources by flooding the system or network with information
  - Since all resources are exhausted others are denied access to the resources
- Distributed DoS (DDoS) attacks are coordinated denial of service attacks involving several people and/or machines to launch attacks

Denial of Service (DoS) Attack

Types:

1. Ping of Death
2. SSPing
3. Land
4. Smurf
5. SYN Flood
6. CPU Hog
7. Win Nuke
8. RPC Locator
9. Jolt2
10. Bubonic
11. Microsoft Incomplete TCP/IP Packet Vulnerability
12. HP Openview Node Manager SNMP DOS Vulnerability
13. Netscreen Firewall DOS Vulnerability
14. Checkpoint Firewall DOS Vulnerability

10 common hacking techniques
https://www.youtube.com/watch?v=V3CTfJ2ZP7M
Time: 10:07

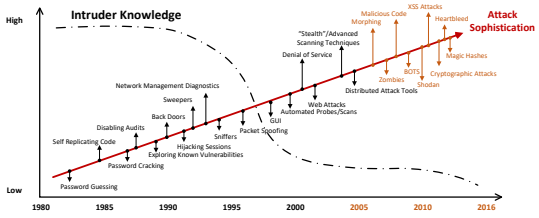
Answer the questions:
What protection mechnisms can you propose against the techniques discussed?

Hacker's tools and protection against them

Newbies and enthusiastic activists didn't realize that many automatic tools available on Internet could provide hacker's personal information to investigators.

For example, the Low Orbit Ion Cannon tool used by Anonymous to launch distributed denial of services attacks didn't mask user IP addresses, making them easier to find. The Low Orbit Ion Cannon allowed users to form a voluntary botnet to launch distributed denial of service attacks against companies severing times with WikiLeaks. The tool did not conceal the user IP address.

Hacker's tools: Is it easy to become a hacker?



Script Kiddie Hacking Tools

- various tools that are classified as too easy to use, or too automated and these fall into the category of Script Kiddie Tools.
- Examples of these tools would mainly be password cracking tools:
  - Cain and Abel Password Cracker,
  - Brutus Password Cracker and
  - John the Ripper for Password Cracking.
- More complicated
  - **Karkinos – Beginner Friendly Penetration Testing Tool**
  - **zANTI – Android Wireless Hacking Tool**

Comparison of Best Hacking Tools -1

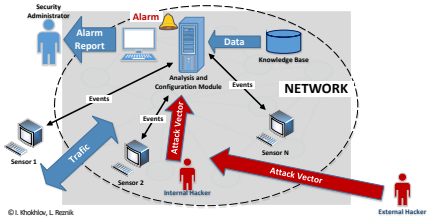
Tool Name	Platform	Best For	Type	Price
Acunetix	Windows, Mac, RedHat 8, etc. & Web-based.	End-to-end web security scanning.	Web Application Security Scanner.	Get a quote.
Netsparker	Windows & Web-based	Accurate and automated application security testing.	Web Application Security for Enterprise.	Get a quote
Intruder	Cloud-based	Finding & fixing vulnerabilities in your infrastructure.	Computer & Network security.	Free monthly trial available. Pricing starts from $38/month.
Nmap	Mac OS, Linux, OpenBSD, Solaris, Windows	Scanning network.	Computer security & Network management.	Free

Source: https://www.softwaretestinghelp.com/ethical-hacking-tools/ accessed on 10/25/2021

Comparison of Best Hacking Tools -2

Tool Name	Platform	Best For	Type	Price
Metasploit	Mac OS, Linux, Windows	Building anti-forensic and evasion tools.	Security	Metasploit Framework: Free. Metasploit Pro: Contact them.
Aircrack-Ng	Cross-platform	Supports any wireless network interface controller.	Packet sniffer & injector.	Free
Wireshark	Linux, Windows, Mac OS, FreeBSD, NetBSD, OpenBSD	Analyzing data packets.	Packet analyzer	Free
Ettercap	Cross-platform	It allows you to create custom plugins.	Computer security	Free

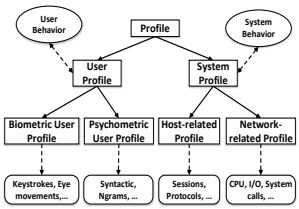
Protection: Hacker's Intrusion Detection System (IDS)



Anomaly IDS Based on Profiling

Works similarly to immune system of living organisms:

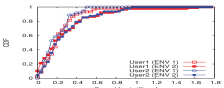
- Detect intrusions by identifying suspicious changes in a user or system-wide activities.
- System health factors:
  - Performance
  - Use of system resources
- User factors:
  - User's biometrics
  - User's behavior
- Multi-layered protection
- Distributed detection
- Diversity of detection
- Inexact matching ability
- Detection of unseen attacks



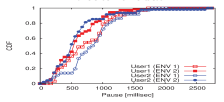
Source: Peng, J., Choo, K.K.R. and Ashman, H., 2016. User profiling in intrusion detection: A review. *Journal of Network and Computer Applications*, 72, pp.14-27.

Anomaly IDS Based on User Profiling

- Can detect hacker attack on early stage, before attack becomes successful.
- Uses biometrics for detecting anomalies in user's behavior:
  - Keystrokes
  - Pointer (mouse, touchpad, touchscreen) usage
  - Face recognition
  - Iris recognition
  - Retina recognition
  - Fingerprint recognition
  - Voice recognition



Speed metric plotted for two different users under two different environments each.



Pause-and-Click metric plotted for two different users under two different environments each.

Image source: Zheng, N., Paloski, A. and Wang, H., 2016. An efficient user verification system using angle-based mouse movement biometrics. *ACM Transactions on Information and System Security (TISSEC)*, 18(3), p.11.

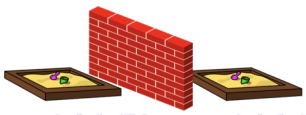
IEEE WCCI 2020
IEEE World Congress on Computational Intelligence
Virtual Conference – July 19-24, 2020

USE CASE: RECURRENT NEURAL NETWORKS FOR COLLUDED APPLICATIONS ATTACK DETECTION IN ANDROID OS

Igor Khokhlov, Ninad Ligade, Leon Reznik
Rochester Institute of Technology
Rochester, NY, USA
ixk8996@rit.edu, nl4439@rit.edu, lr@cs.rit.edu

Android OS Security Features

Sandboxing



Application UID 1 Application UID 2

Signature

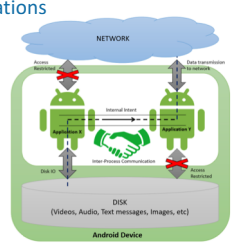
Permissions

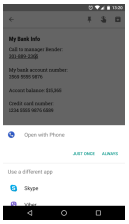
In order to use device's resources, an application should ask for a permission

SPONSORS:

Colluded Applications

Colluded applications – are collaborating applications that can bypass permissions through communicating with each other.





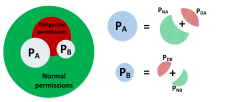
Colluded Applications

Application A and application B are called colluded if application A can access the private data but cannot leak collected data directly, application B does not have access to private data but can leak any collected data, and application A transmits collected data to the *application B* in the background without a user's awareness.

$$(A, B \in S) \wedge (P_{DA}, P_{DB} \subset DP) \wedge (P_{DA} \neq P_{DB}) \wedge (p_D \in P_{DA})$$

$$\wedge (p_D \notin PDB) \wedge (p_L \in PDB) \wedge (p_L \notin P_{DA})$$

$$\wedge t_A(B, D_{p_D}, background) \rightarrow A \text{ and } B \text{ are colluded}$$



Khokhlov I., Perez M., Reznik L., "Machine Learning in Anomaly Detection: Example of Colluded Applications Attack in Android Devices", 18th IEEE International Conference on Machine Learning and Applications - ICMLA 2019, Boca Raton, FL, USA, December 2019 (pp. 1328-1333);
Khokhlov I., Perez M., Reznik L., "System Signals Monitoring And Processing For Colluded Application Attacks Detection In Android OS", 2019 Western New York Image and Signal Processing Workshop, Rochester, NY, USA, October 2019 (pp. 1-5);
Khokhlov I., Reznik L., "Colluded Applications Vulnerabilities in Android Devices", The 15th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC 2017), Orlando, FL, November 2017 (pp. 462-469).

Our Hypothesis

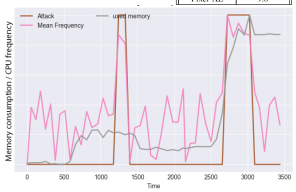
Colluded applications may create distinctive patterns in the memory consumption and CPU usage signals that could be detected with recurrent neural networks techniques application

Empirical study- Data Collection

Signals recorded:
- Overall memory consumption (RAM)
- CPU cores clock speed (CPU frequency)

Scenarios:
- Pure Attack
- No Attack
- No Data Transmission

Name	OS Version
One Plus 6T	9.0
One Plus 5T	8.0
Moto G6	9.0
Moto G5	8.0
Pixel XL	9.0

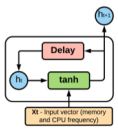


Empirical study - Data Pre-processing

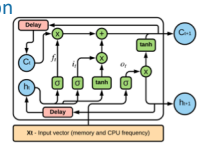
The data pre-processing includes:
- Noise reduction
- Stabilizing the time interval between records
- Data normalization
- Data labeling
- Input dimensionality reduction

$$normalized\ value = \frac{col_{val} - col_{min}}{col_{max} - col_{min}}$$

Attack detection



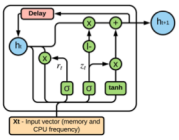
Basic architecture for a simple RNN model



Basic architecture for LSTM model

Layer (type)	Output Shape	Param #
gru_1 (GRU)	(None, 100)	33900
dropout_1 (Dropout)	(None, 100)	0
dense_1 (Dense)	(None, 100)	10100
dense_2 (Dense)	(None, 2)	202

Total params: 44,202
Trainable params: 44,202
Non-trainable params: 0

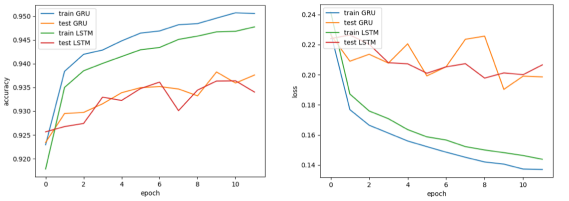


Basic Architecture for GRU model

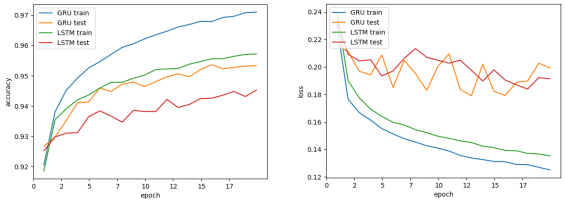
Layer (type)	Output Shape	Param #
gru_1 (GRU)	(None, 100)	33900
dropout_1 (Dropout)	(None, 100)	0
dense_1 (Dense)	(None, 100)	10100
dense_2 (Dense)	(None, 2)	202

Total params: 44,202
Trainable params: 44,202
Non-trainable params: 0

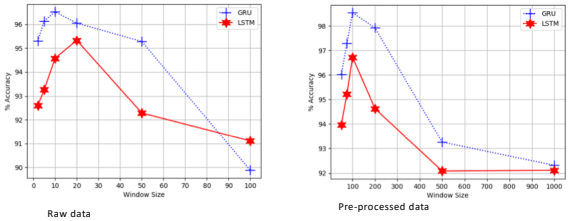
Results – raw data



Results – pre-processed data



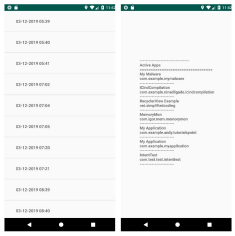
Detection accuracy vs. window size



Raw data

Pre-processed data

Implementation on a real Android smartphone



Based on TensorFlow-Lite model
Android application has three parts:
Service component, and two Activity component

Conclusions

- We developed the “colluded applications” attack definition and conducted an empirical study that exploited this novel attack.
- We developed effective and efficient implementation of the attack detection based on the analysis of the major accessible Android OS system technological signals of mobile devices.
- The attack detector is based on RNN architecture and its variations
- The attack detector is designed to perform in real-time on a stock Android smartphone with no firmware modification required.
- We made the dataset available for public use (link: http://bit.ly/2k3M5Ny)
- The most effective and efficient design is based on the GRU model, which achieved more than 95% accuracy in the attack detection task.
- The developed GRU model was then converted into a stand-alone Android application that detects attacks in real-time