CSCI369 Ethical Hacking

Lecture 6 Privacy Tools, Zero-Day, APT and Ransomware

A/Prof Joonsang Baek

School of Computing and Information Technology

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

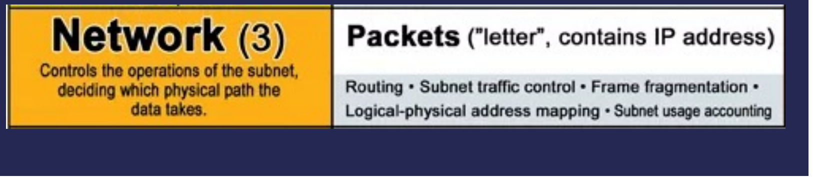
Privacy Tools

- The term “privacy” is a double-edged sword:
  - ➢It can provide a user with a state free from being watched.
  - ➢It can provide a hacker with a tool that can hide their tracks of attack.
- Anonymity: Providing privacy does not always mean providing anonymity but anonymity is an essential part of privacy.

Privacy Tools

- Virtual Private Network (VPN)
  - ➢All the IP packets from the source (hacker) and a VPN server are encrypted through *IPSec*.
    - ✓Originally VPN was created for employees to securely connect to their company's network remotely.
  - ➢All internet activity of the hacker is routed through the VPN server.
  - ➢VPN can hide the hacker's physical location.
  - ➢VPN can give the hacker anonymity if configured properly.

IPSec

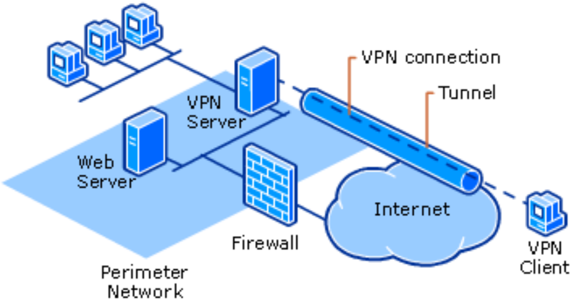


Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	Packets ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting

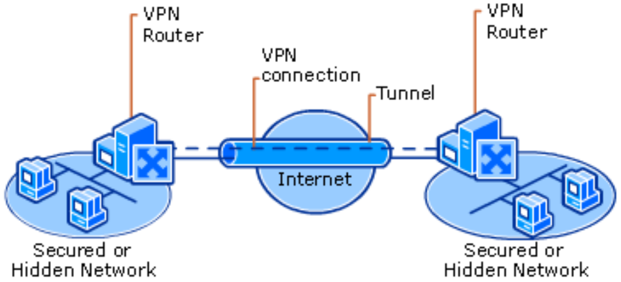
- Acronym for **I**nternet **P**rotocol **Sec**urity
- IPSec is a framework of open standards that provides, between participating peers at the **IP layer** with
  - ➢ data confidentiality
  - ➢ data integrity
  - ➢ and data authentication.
- IPsec can protect data flows between
  - ➢a pair of hosts (*host-to-host*),
  - ➢between a pair of security gateways (*network-to-network*),
  - ➢or between a security gateway and a host (*network-to-host*).

IPSec

- Example of protected data flow



Network-to-Host



Network-to-Network

- Most popular application of IPSec is a Virtual Private Network (VPN).
- Many company uses VPN because it is much cheaper than building a dedicated private network.
- It is also a good privacy tool not only for hackers, but also general users.

Privacy Tools

- Using Tor network
  - Tor: A group of volunteered servers which can be used to provide anonymity on the Internet.
  - Tor users use the Internet by connecting through a series of virtual tunnels rather than making a direct connection.
  - Tor is used as an effective censorship circumvention tool, allowing its users to reach otherwise blocked destinations or content → In fact, it was first invented by US military.

Privacy Tools

- How Tor works
  - To create a private network path using Tor, the user's Tor software or client builds a virtual circuit of encrypted connections, called “Onion Routing” one by one through nodes on the network.
  - The circuit is extended one hop at a time, and each node knows only which node gave it data and which node it is giving data to → No individual node ever knows the complete path that a data packet has taken.
  - The client (source) negotiates a separate set of encryption keys for each hop along the circuit to ensure that each hop can't trace these connections as they pass through.

Privacy Tools

- Features of Tor
  - ➢Once a Tor routing has been established, various types of data can be exchanged.
  - ➢It is also possible several different sorts of software applications can be deployed over the Tor network.
  - ➢Because each node sees no more than one hop in the circuit, neither an eavesdropper nor a compromised node can use traffic analysis to link the connection's source and destination.
- Implementations
  - ➢Tor Browser, Tor Messenger etc.

Privacy Tools

- Limitation
  - ➢Tor has been very effective but research has been doing to break Tor by compromising Tor nodes.
  - ➢User's misconfiguration can lead to compromise of anonymity.

Privacy Tools

- DNS (Domain Name Service) Encryption
  - ➢A DNS query/response leaks the information about the sites the user is communicating with. → Privacy issues arise.
  - ➢The Internet Service Provider (ISP) (or third party) can *snoop* the entries in the DNS server it is running.
  - ➢Therefore, DNS encryption is proposed:
    - ✓DNS over HTTPS (proposed by Google): Encrypt all the DNS queries/responses through TLS.
    - ✓OpenDNS (proposed by Cisco): Similar to DNS over HTTPS (https://www.opendns.com/about/innovations/dnscrypt/).

Privacy Tools

- Anonymous-friendly Search Engines
  - ➢Every major search engine (Google, Yahoo! and Bing) online today tracks almost 100% of searches the users perform.
  - ➢if you want to use a search engine that doesn't, consider to use alternative anonymous-friendly Search Engines –DuckDuckGO and Startpage.
  - ➢*DuckDuckGo*: The main approach that this search engine takes to protect user privacy is in not using the filtering system that major search engines use to offer "personalized results".

Privacy Tools

- *Private browsing mode*: Chrome and Firefox browser provides this mode. All search and browsing history will be cleared once the user quits the browser.

Privacy Tools

- Other methods of protecting a hacker’s identity
  - ➢Change MAC address.
  - ➢Use public WiFi with VPN.
    - ✓Using public WiFi without VPN is actually very dangerous.
  - ➢Boot a machine from a “live CD” (running totally in the RAM).
    - ✓Do not leave any logs in your machine.

Zero-Day= Zero-Day Vulnerability/Exploit

- Zero-day vulnerability
  - ➢It refers to a security hole in software that is yet known to the public including software vendors or to antivirus vendors.
  - ➢Although the vulnerability is not yet publicly known, it may already be known by attackers who are quietly exploiting it.
  - ➢Because zero-day vulnerabilities are unknown to software vendors and to antivirus firms, there is no patch available yet to fix the hole and generally no antivirus signatures to detect the exploit.

Zero Day= Zero-Day Vulnerability/Exploit

- Zero-day exploit
  - ➢Zero-day exploit refers to code that attackers use to take advantage of a zero-day vulnerability.
  - ➢Attackers use the exploit code to plant a virus, Trojan horse or other malware onto a computer or device.
  - ➢Zero-day exploit codes are extremely valuable and are used not only by criminal hackers but also by nation-state spies and cyber warriors, like those working for the NSA and the U.S. Cyber Command.

Zero Day Markets

- Expected or not, zero-day exploits are traded in
  - Black market where criminal hackers trade in exploit code and vulnerability information to break into systems;
  - White market where researchers and hackers disclose vulnerability information to vendors, in exchange for money;
  - Gray market where some defense contractors sell zero-day exploits and vulnerability information to militaries, intelligence agencies and law enforcement to use for surveillance and offensive computer operations.

Advanced Persistent Threat (APT)

- Definition of APT according to NIST
  - "*An adversary that possesses <u>sophisticated levels of expertise and significant resources</u> which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include <u>establishing and extending footholds</u> within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future.*"

APT Characteristics

- Specific targets and clear objectives
  - ➢The targets of APT are typically governments or organizations possessing substantial digital assets.
  - ➢The top ten industry vertical targets are education, finance, high-tech, government, consulting, energy, chemical, telecom, healthcare and aerospace.
  - ➢While traditional attacks propagate as broadly as possible to improve the chances of success and maximize the harvest, an APT attack only focuses on its pre-defined targets, limiting its attack range.
  - ➢APTs typically look for digital assets that bring competitive advantage or strategic benefits, such as national security data, intellectual property, trade secrets, etc.

APT Characteristics

- Highly organized and well-resourced attackers
  - ➢The actors behind APTs are typically a group of skilled hackers, working in a coordinated way.
  - ➢They may work in a government or military cyber unit, or be hired as contractors by governments and private companies.
  - ➢They are well-resourced from both financial and technical perspectives. This provides them with the ability to work for a long period, and have access to zero-day vulnerabilities and attack tools. When they are state-sponsored, they may even operate with the support of military or state intelligence.

APT Characteristics

- A long-term campaign with repeated attempts
  - ➢An APT attack is typically a long-term campaign, which can stay undetected in the target's network for several months or years.
  - ➢APT actors persistently attack their targets and they repeatedly adapt their efforts to complete the job when a previous attempt fails.
  - ➢This is different from traditional threats, since traditional attackers often target a wide range of victims, and they will move on to something less secure straight way if they cannot penetrate the initial target.

APT Characteristics

- Stealthy and evasive techniques
  - ➢APT attacks are stealthy, possessing the ability to stay undetected, concealing themselves within enterprise network traffic, and interacting just enough to achieve the defined objectives.
  - ➢For example, APT actors may use zero-day exploits to avoid signature-based detection, and encryption to obfuscate network traffic. This is different from traditional attacks, where the attackers typically employ "smash and grab" tactics that alert the defenders.

Phases of APT

- A typical APT attack will have the following six phases:
  (1) Reconnaissance
  (2) Delivery
  (3) Initial intrusion
  (4) Command and control
  (5) Lateral movement
  (6) Data exfiltration

Examples of APT

- Stuxnet
  - ➢Stuxnet is a worm, often classified as an APT malware.
  - ➢Designed to attack programmable logic controllers of nuclear centrifuges.
  - ➢It is believed to have ruined almost 20 percent of Iran's nuclear centrifuges.
- Duqu
  - ➢Many experts suspect that it is related to Stuxnet.
  - ➢It was designed to gather information that could be used to attack SCADA systems.
- Flame
  - ➢Used for reconnaissance and information gathering in the Middle East: Record audio, screen, keyboard activities, Skype conversations.
  - ➢The size is large: Around 20 megabytes.
  - ➢Spread through USB → Known to be the most advanced malware.

Stuxnet

- SCADA (Supervisory Control and Data Acquisition)
  - ➢A control system architecture designed to control processes and automation in factories and power plants with two roles:
  - ➢High-level management
    - ✓Computers, networked data communications and GUIs for supervisory process
  - ➢Low-level interface
    - ✓Peripheral devices such as programmable logic controllers (PLC).
    - ✓PLC : Industrial digital computer for controlling manufacturing processes

Stuxnet

- The Stuxnet worm is designed to attack the "SCADA" software
  - ➢It is unusual to focus on attacking industry-related systems, which is one of the reasons that the Stuxnet worm was developed by a well-resourced organisation (perhaps related to some governments).
- It has been known that the Stuxnet targets nuclear facilities in Iran.
- Symptoms
  - ➢The worm was designed to hop from PCs to the Siemens PLCs used for SCADA process control.

Stuxnet

- ➢Once a SCADA computer is infected, the worm modifies the data sent by the sensors to the central monitors in such a way that the operation of centrifuges (used for uranium enrichment) gradually malfunctions while human operators are not aware of it. → *The worm gradually raises the frequencies of rotation of centrifuge to a level that it will break*.

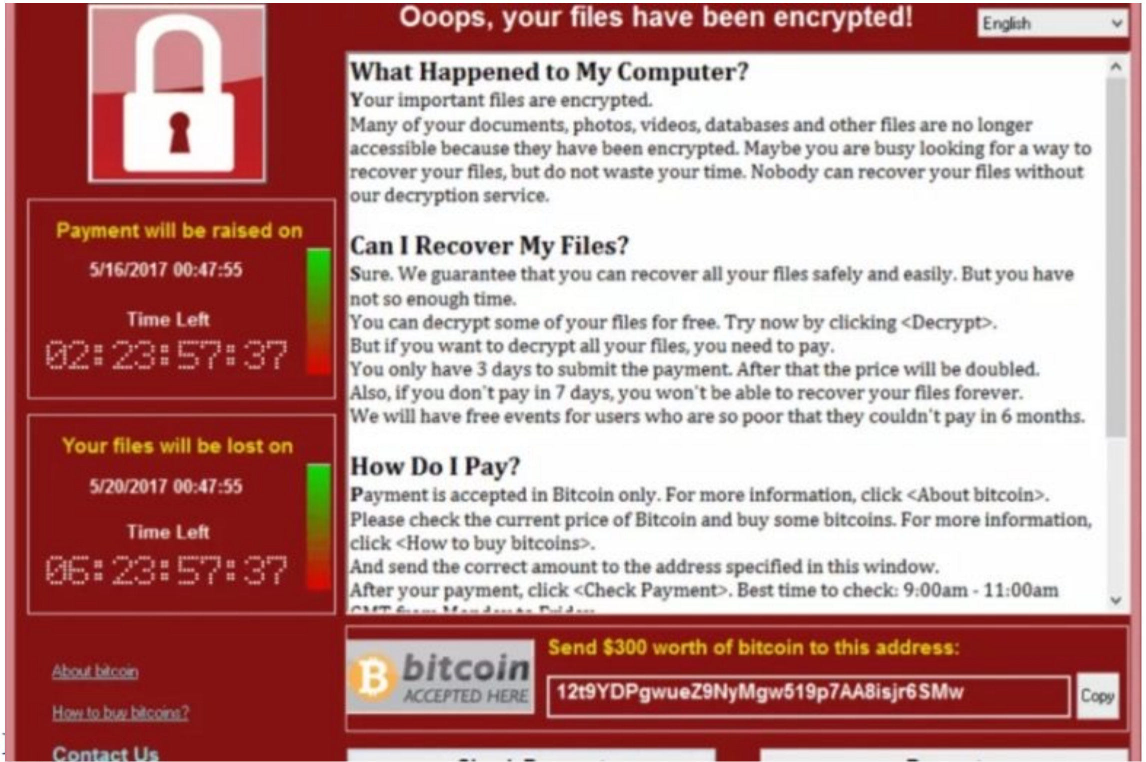
- Stolen certificate
  - ➢Some of the drivers of the Stuxnet worm used valid signed certificates from RealTek (a semiconductor company in Taiwan) and another company near RealTek.
  - ➢It seems that a private signing key could have been compromised.
  - ➢This shows that the Stuxnet worm was developed by an entity which has good resources.

Stuxnet

- Analysis: Why is Stuxnet APT?
  - ➢Recap: The four characteristics of APT:
  - (1) Specific targets and clear objectives
    - ✓Yes, as Stuxnet has a clear target.
  - (2) Highly organized and well-resourced attackers
    - ✓Yes, all the attack/propagation methods are highly sophisticated.
  - (3) A long-term campaign with repeated attempts
    - ✓Yes, it there are a few ways to attack. It uses Conficker's method too.
  - (4) Stealthy and evasive attack techniques
    - ✓Yes, the malfunction of centrifuges was gradual (not abrupt).

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Ransomware



What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Ransomware

- Ransomware
  - ➢Ransomware is a type of malware that threatens to publish the victim's data or permanently block access to it unless a ransom is paid.

  - ➢Usually recent ransomware uses an advanced technique called cryptoviral extortion, in which it encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Ransomware

- Ransomware (continued)
  - ➢In a properly implemented cryptoviral extortion attack, recovering the files without the decryption key is **intractable** – and it is very difficult to trace digital currencies, which are used for the ransoms, making tracing and prosecuting the attacker difficult
  - ➢The concept of file encrypting ransomware was invented and implemented by Young and Yung at Columbia University and was presented at the 1996 IEEE Security & Privacy conference

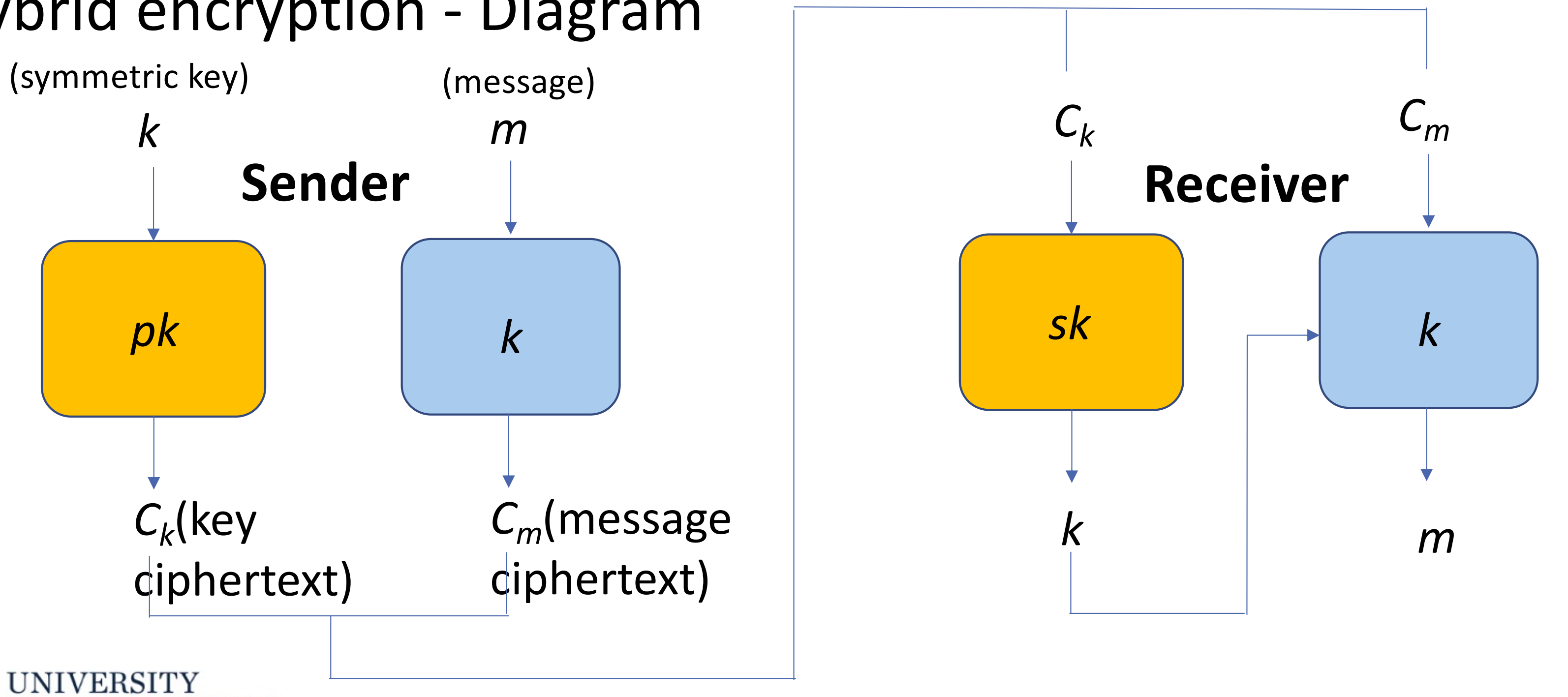
UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Operation of Ransomware

- Preliminary: Hybrid encryption
  - ➢In reality, it is expensive to encrypt a large file using a public key encryption algorithm
    - ✓The security of most public key encryption algorithms is based on computationally-hard mathematical problems like integer factorization → The computational cost is high
  - ➢The solution is to generate a “symmetric” key to encrypt a message using a symmetric encryption algorithm and encrypt the symmetric key using a public key encryption algorithm
  - ➢Both the ciphertext that encrypts the symmetric key and the ciphertext that encrypts the message will be sent to the receiver (who owns the matching private key)

Operation of Ransomware

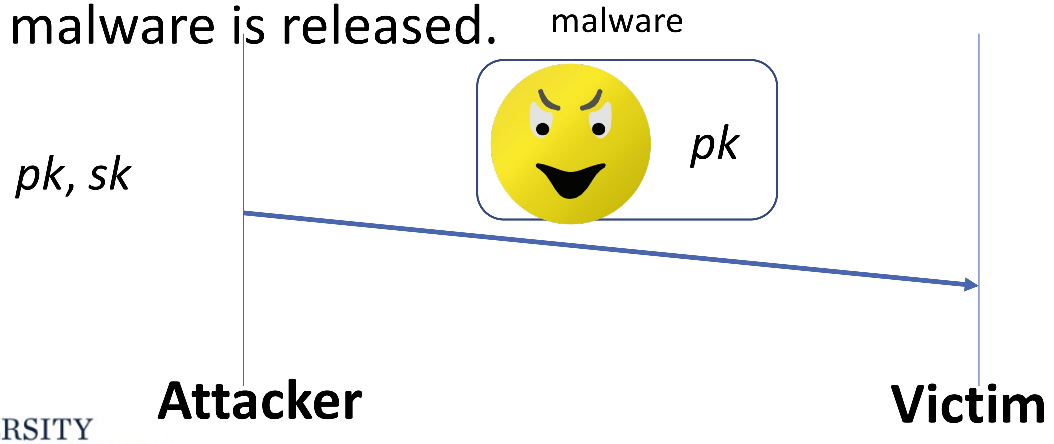
- Hybrid encryption - Diagram



UNIVERSITY OF WOLLONGONG AUSTRALIA

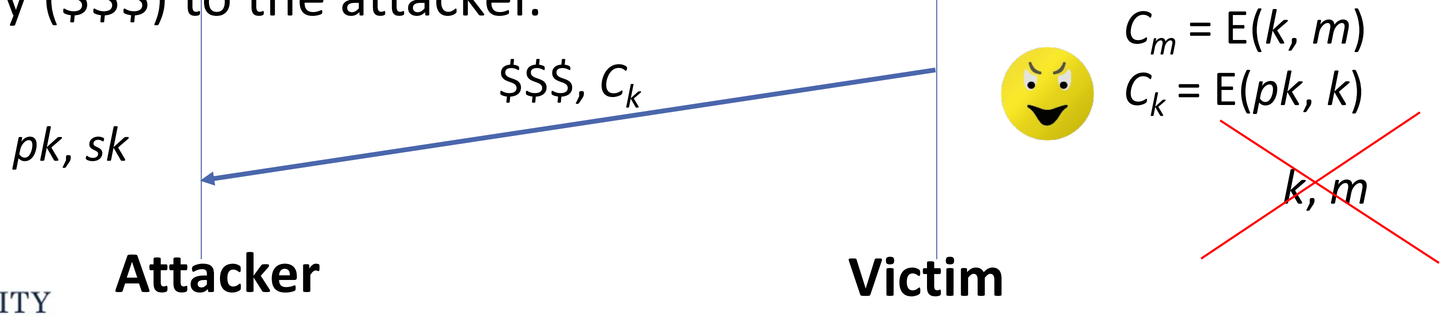
Operation of Ransomware

- Ransomware is the following three-round protocol carried out between the attacker and the victim.
  - ➢Step 1: The attacker generates a public and private key pair (*pk*, *sk*) and places the corresponding public key (pk) in the malware. The malware is released.



Operation of Ransomware

- Step 2: To carry out the attack, the malware generates a random symmetric key (*k*) and encrypts the victim's data (*m*) to create C_m(message ciphertext). It also encrypts *k* with the attacker’s public key *pk* to create C_k (key ciphertext). It then **deletes** both *k* and *m* to prevent recovery. It displays a message explaining how to pay the ransom. The victim then sends the key ciphertext C_k and e-money ($$$) to the attacker.



$C_m = \mathrm{E}(k, m)$

$C_k = \mathrm{E}(pk, k)$

$\cancel{k, m}$

$\$\$\$, C_k$

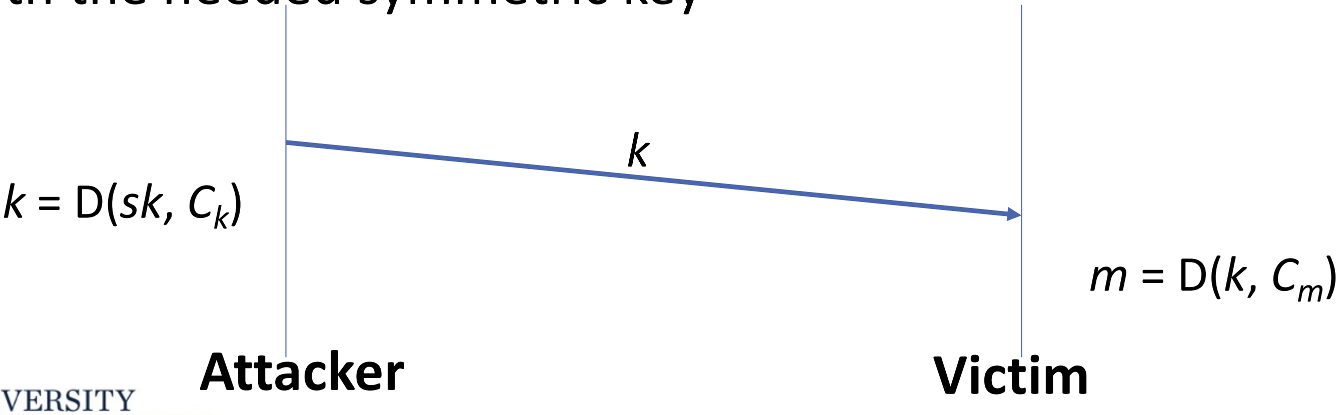
pk, *sk*

Attacker

Victim

Operation of Ransomware

- Operation of ransomware (continued)
  - ➢Step 3: Once the attacker receives the payment, he/she will decrypt C_k with the attacker's private key, and sends the symmetric key k to the victim. The victim decrypt the message ciphertext C_m with the needed symmetric key



Operation of Ransomware

- Why the attack makes sense:
  - ➢Because the symmetric key is randomly and independently generated with the output size at least 128 in bits, any other key cannot help the victim decrypt the encrypted file
  - ➢The attacker's private key will not be exposed to victims
  - ➢The victim need only send a very small ciphertext (the encrypted symmetric-cipher key) to the attacker so the ransom transaction can be efficient

Types of Ransomware

- Non-encrypting ransomware
  - ➢Does not use encryption but by limiting access to some services or deceiving users to pay ransom by making a call or send SMS (such as "Windows Product Activation"), which result in high cost
- Leakware
  - ➢Threatens to publish a victim's data unless a ransom paid
- Mobile ransomware
  - ➢Gains popularity recently
  - ➢Usually they block users (to access) rather than encrypt files
  - ➢Typically targets Android phones → They usually allow applications to be installed from third-party sources

Ransomware Examples

- CryptoLocker (2013)
  - ➢Uses 2048 RSA-bit key → Theoretically impossible to recover the encryption key without private key once locked
  - ➢Targets files with specific extension
  - ➢Payment with Bitcoin or cash voucher is demanded within 3 days after infection
  - ➢Propagated through email attachments and Gameover Zeus botnet
  - ➢Approx. $3 million damages were resulted
  - ➢After Gamenover Zeus botnet is captured by Operation Tovar, the spread was stopped.

Ransomware Examples

- CryptoLocker.F (2014)
  - ➢Targets Australian users (but it seems unrelated to the original CryptoLocker)
  - ➢Propagated through a fraudulent email claiming a failed delivery notice from Australia Post → Users are tricked to download the ransomware payload through clicking the link in email
  - ➢Computers in Sydney studio of ABC were infected

Ransomware Examples

- WannaCry (2017)
  - ➢Propagated through the leaked EternalBlue, which had been developed by NSA to exploit SMB protocol on Windows
  - ➢Infected near 230,000 machined around the world including those in the British National Health Service (NHS), FedEx, Deutsche Bahn and Honda
  - ➢Not confirmed but believed to attributed to North Korea