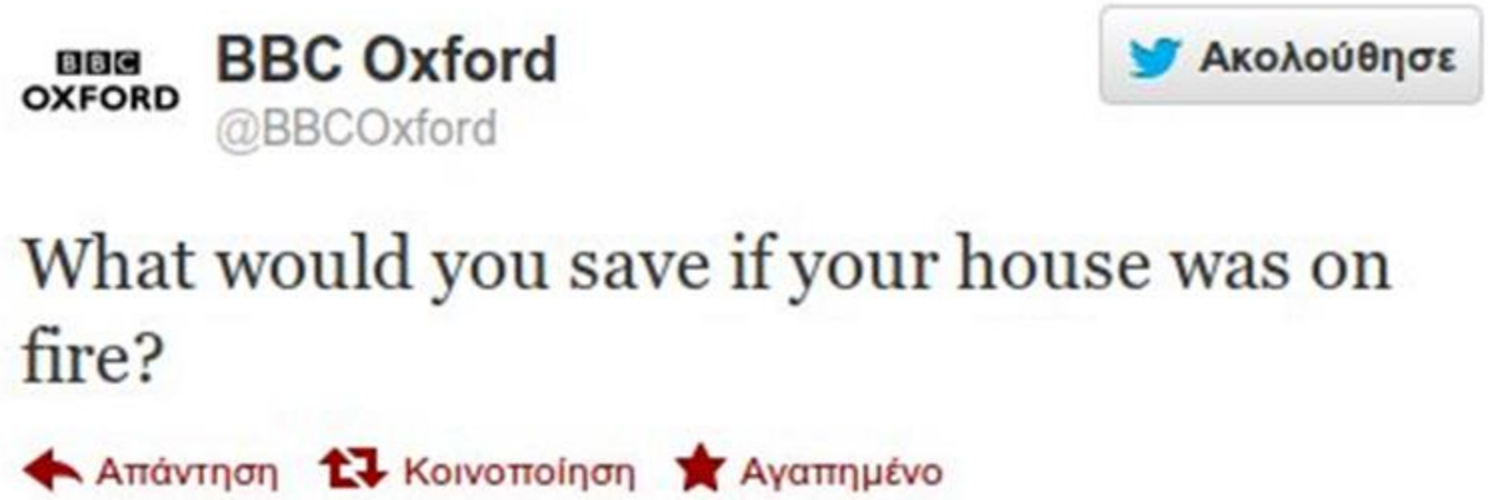
MSc - Cybersecurity

CMT310: Developing Secure Systems and Applications

CIA, Threats & Attacks, and Usability Security

Dr Neetesh Saxena
saxenan4@cardiff.ac.uk

What would you save?



What would you save?

What is Security?

“Treat your password like your toothbrush. Don't let anybody else use it, and get a new one every six months.”

- Clifford Stoll

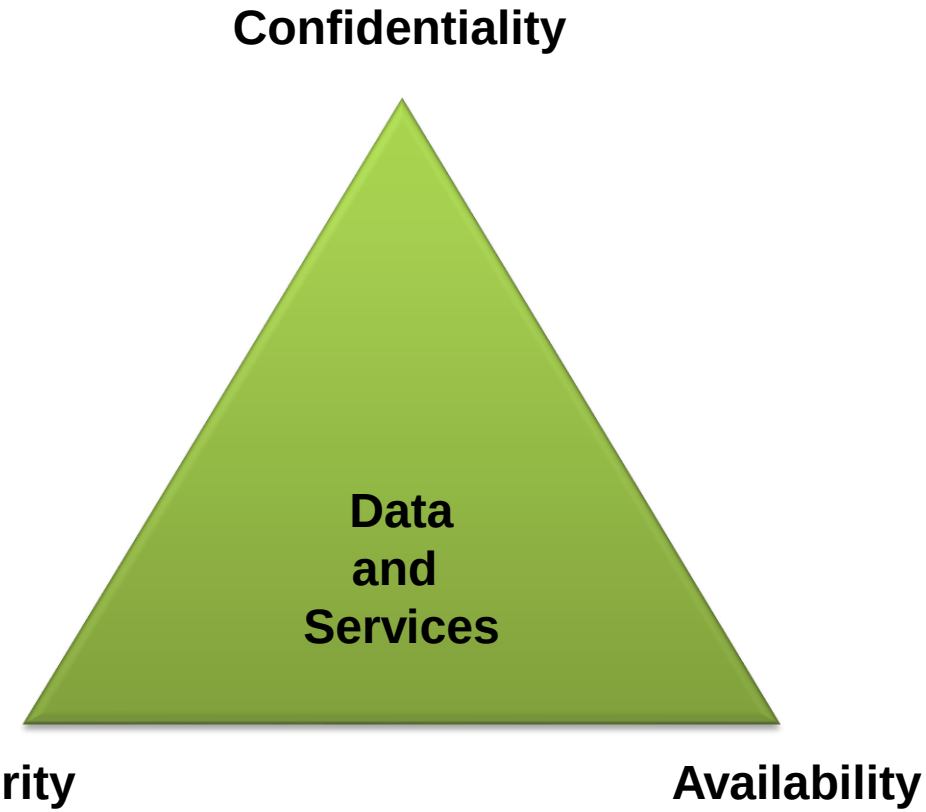
“If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.”

- *Bruce Schneier*

Security Goals – Security Triad

CIA - equal weightage?

CIA – applications?



Confidentiality

"Information is not disclosed to any parties other than the intended recipients."

- Security mechanisms:
  - cryptography
  - access control

- Detection of a breach of confidentiality is very difficult in the digital world, sometimes impossible.

Integrity

"Protection against unauthorised modifications to the data or the system"

- Security mechanisms:
  - cryptography (hash/MAC)
  - error detection/correction codes, checksum
  - establish procedures for system operation, maintenance and administration.

- Integrity violations can be detected most of the time.

Availability

"The information and system resources are available to the legitimate users"

- Security mechanisms:
  - redundancy
  - fault tolerance and resilient system design

- Attacks against the availability of a system are known as 'Denial of Service' attacks (DoS)
- High availability is very expensive

- e.g., Single point of failure -> high availability.
- e.g., Business continuity -> mission critical applications or systems.

Authentication

“Provides the means to verify the identity of an entity”

- An entity can be a person, a computer, or any object on the network, including data.

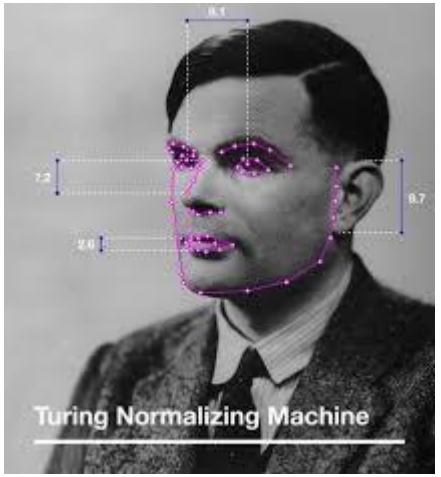
Authentication

3 factors:

- ‘what you know’ – passwords, passphrases, etc.
- ‘what you posses’ – badges, smart cards, tokens.
- ‘what you are’ - biometrics

What you know

What you have



What you are

Non-Repudiation

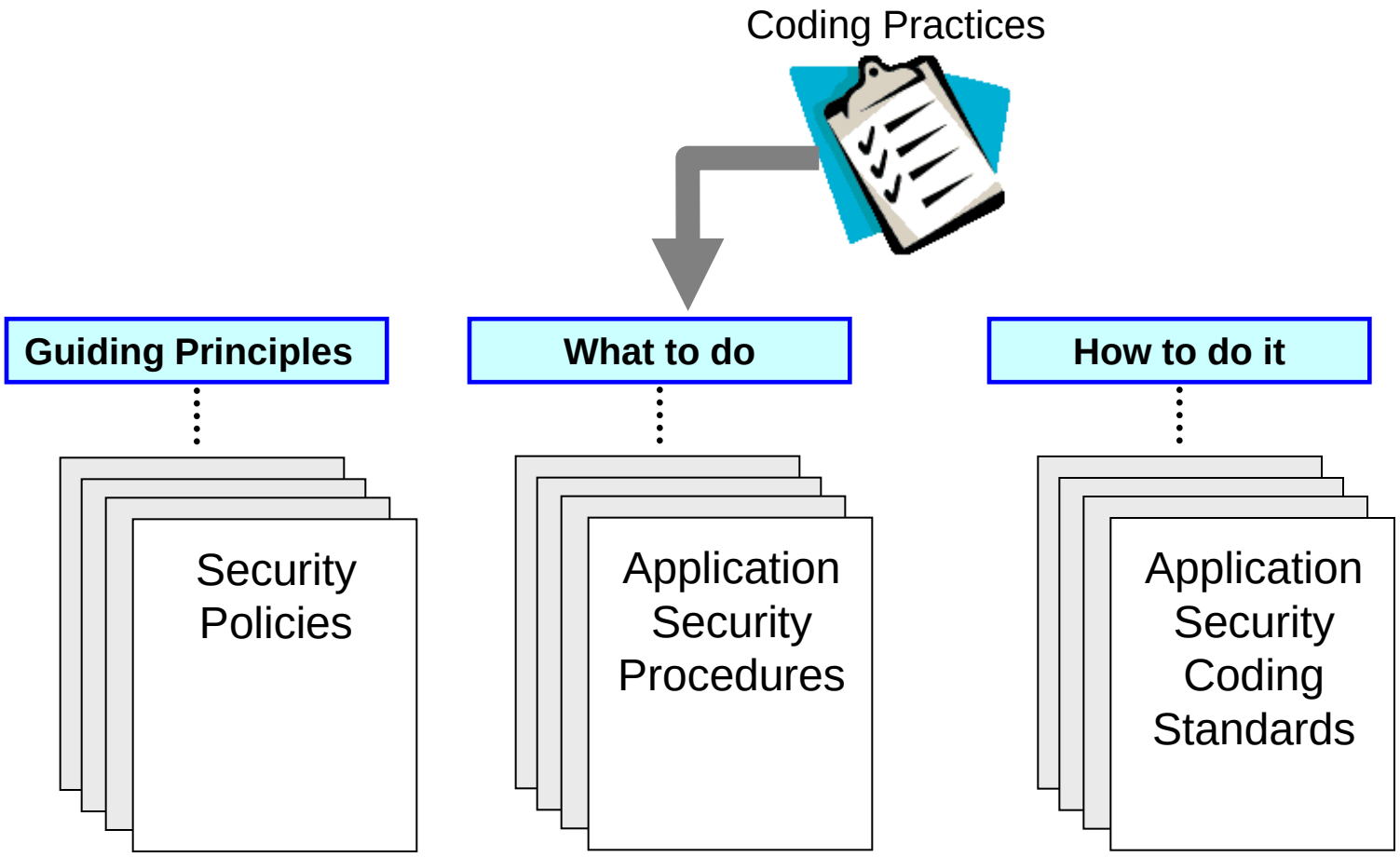
“An entity cannot deny of performing some action”

- Non-repudiation of origin
  - A sender cannot deny that he sent a message
- Non-repudiation of delivery
  - A receiver cannot deny that he received a message

Secure Coding/Programming

- Practice of developing computer software
  - that guards against the security vulnerabilities.
- Defects, bugs and logic flaws are
  - the primary cause of commonly exploited software vulnerabilities.
- Most vulnerabilities stem from
  - a relatively small number of common software programming errors.
- Identify the insecure coding practices
  - and educating developers on secure alternatives.

Developing Guidance Documents



Support Secure Development Lifecycle

What to do

Application Security Requirements

Coding Practices

How you should do it

Application Development Practices

Standardized Libraries

Standard Guidance for non-Library Solutions

What you did

Review Solutions

Did it work

Test Solution Implementation

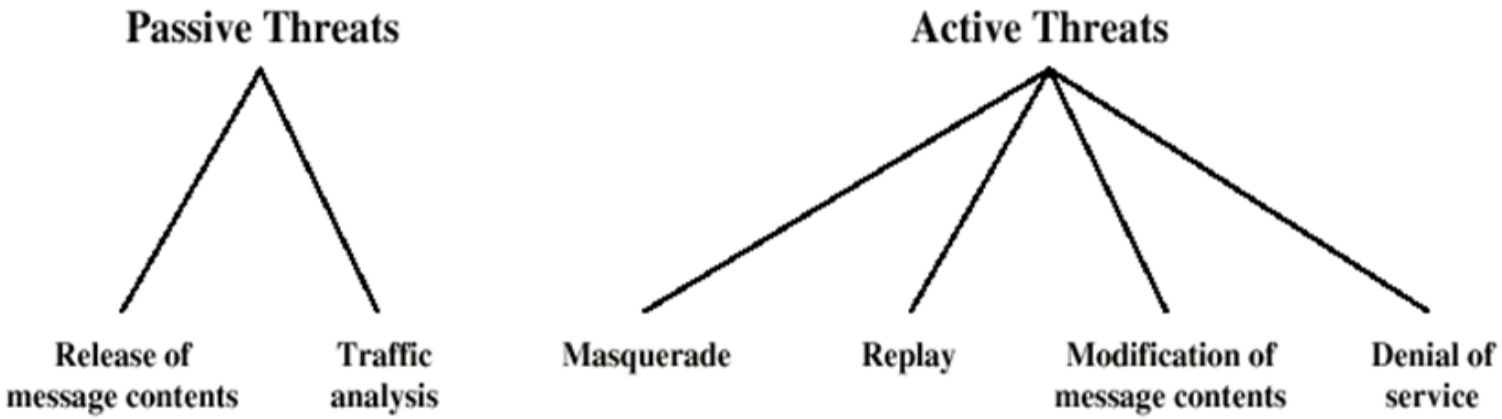
Threat, Vulnerability, and Attack

- A threat is an element which can potentially cause harm or loss
- Threats can be human or non-human

- A vulnerability is a weakness that makes it possible for a threat to occur

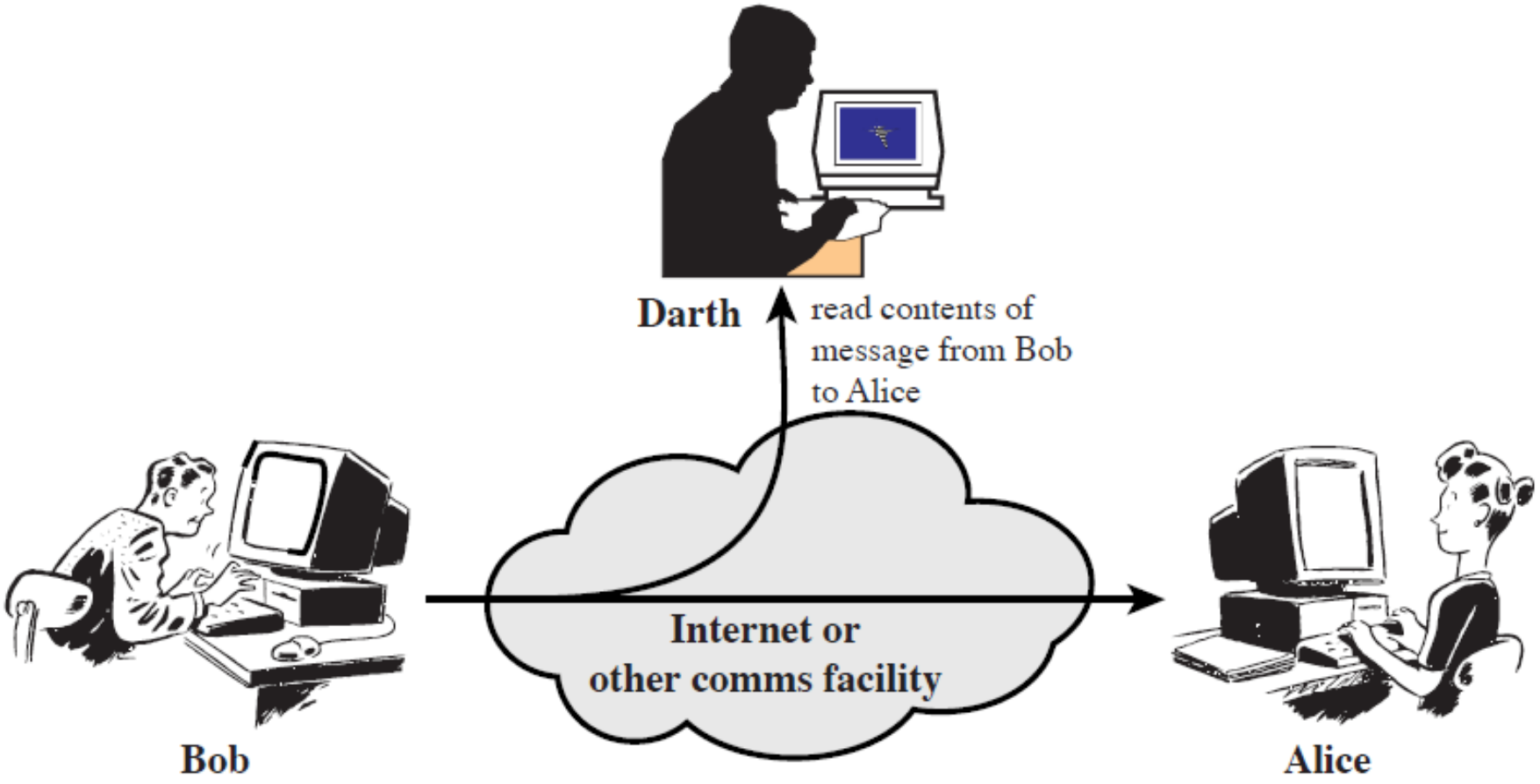
- An attack is any action by a **threat** exploiting a **vulnerability** in order to cause harm or loss

Active and Passive Threats



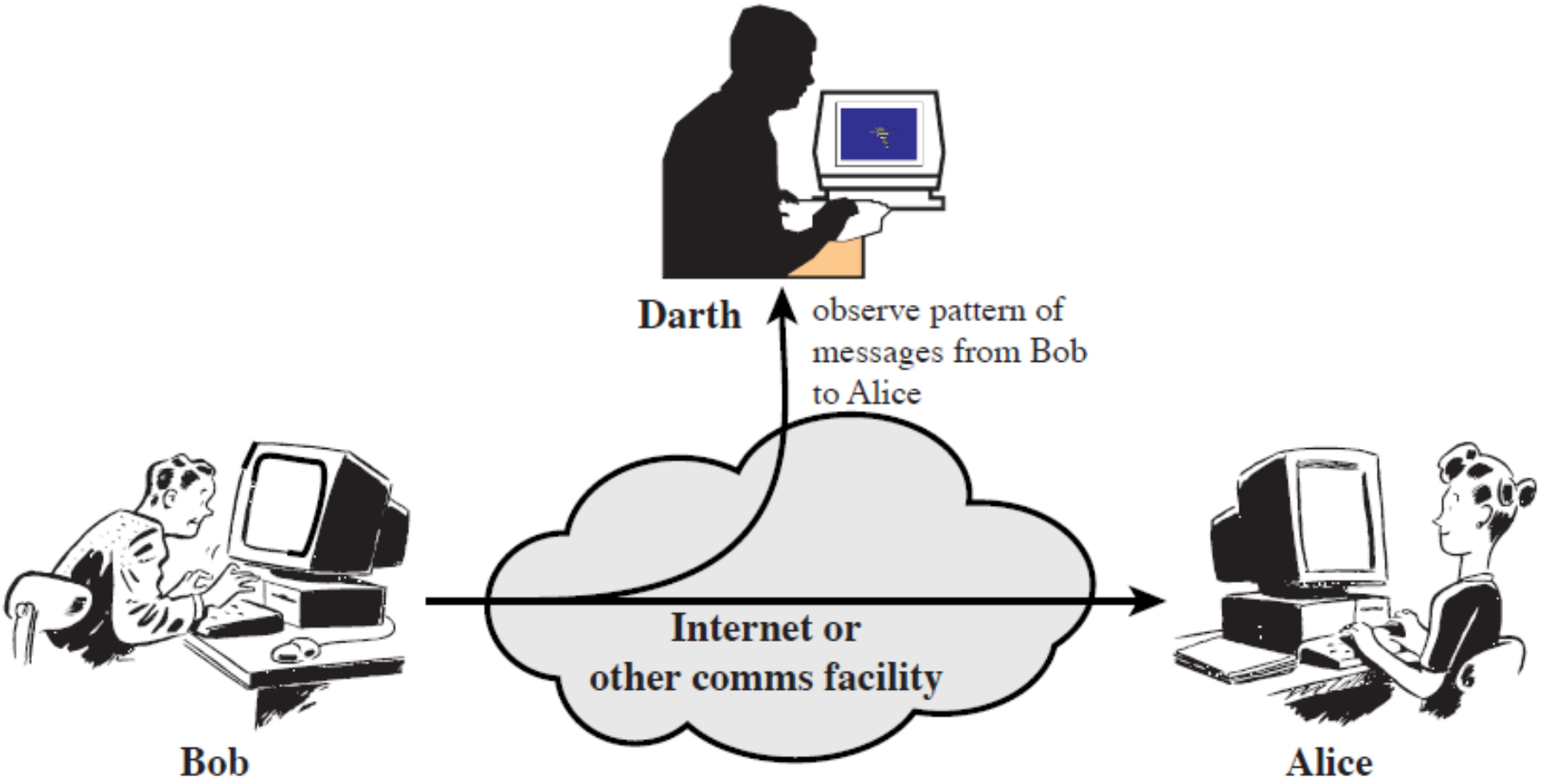
Active and Passive Security Threats

Passive Attack - Eavesdrop



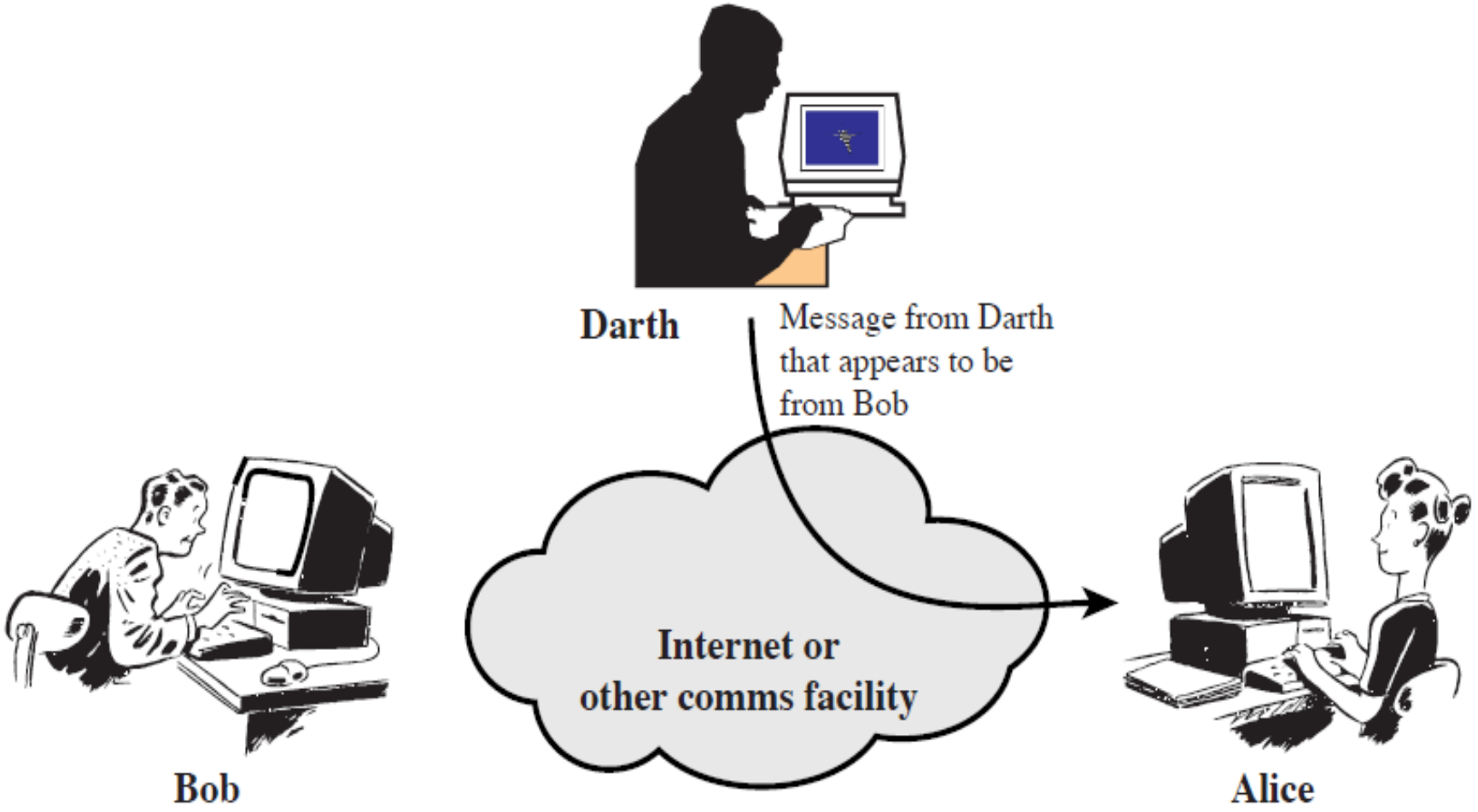
(a) Release of message contents

Passive Attack - Analysis



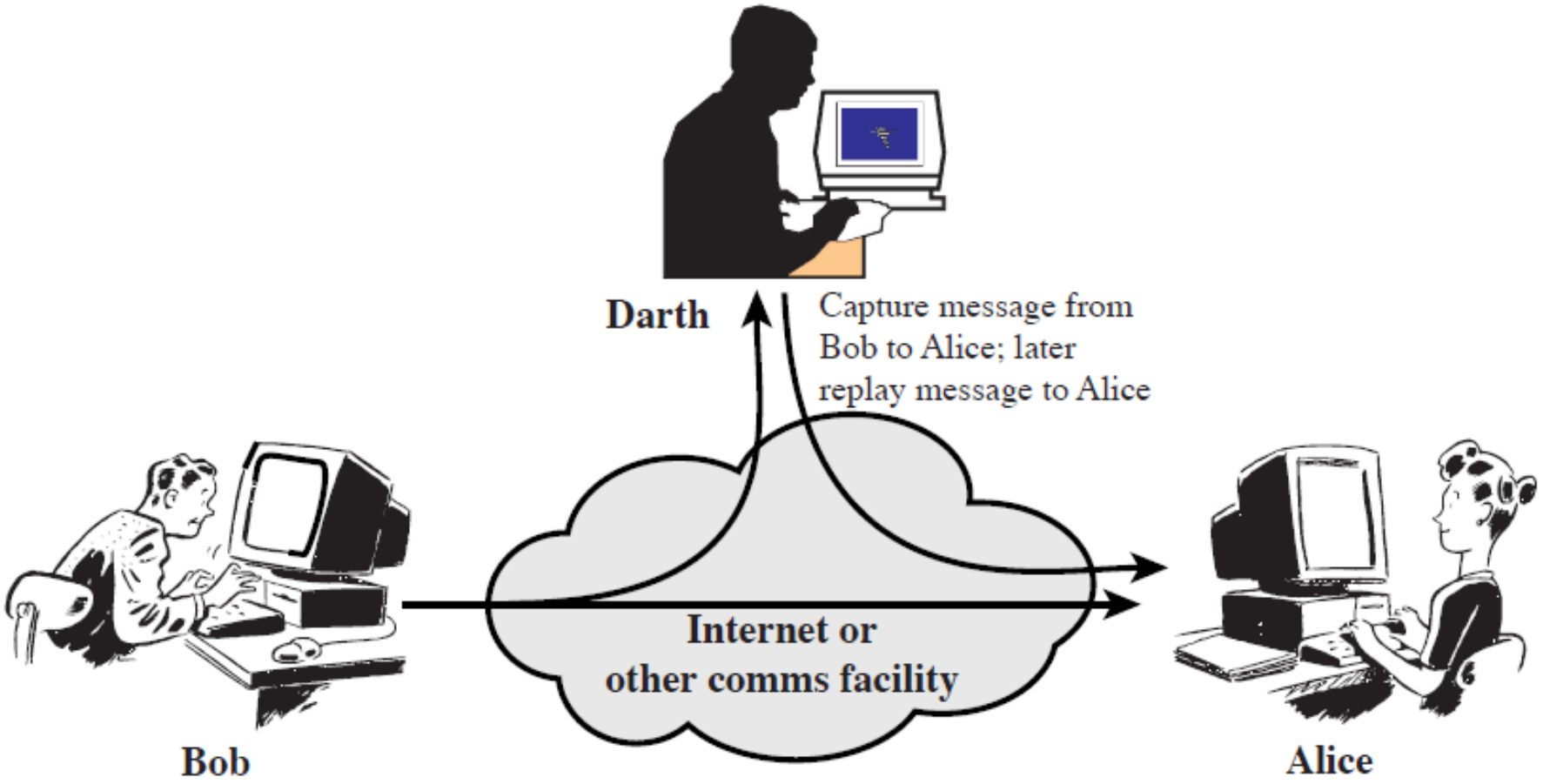
(b) Traffic analysis

Active Attack - Impersonation



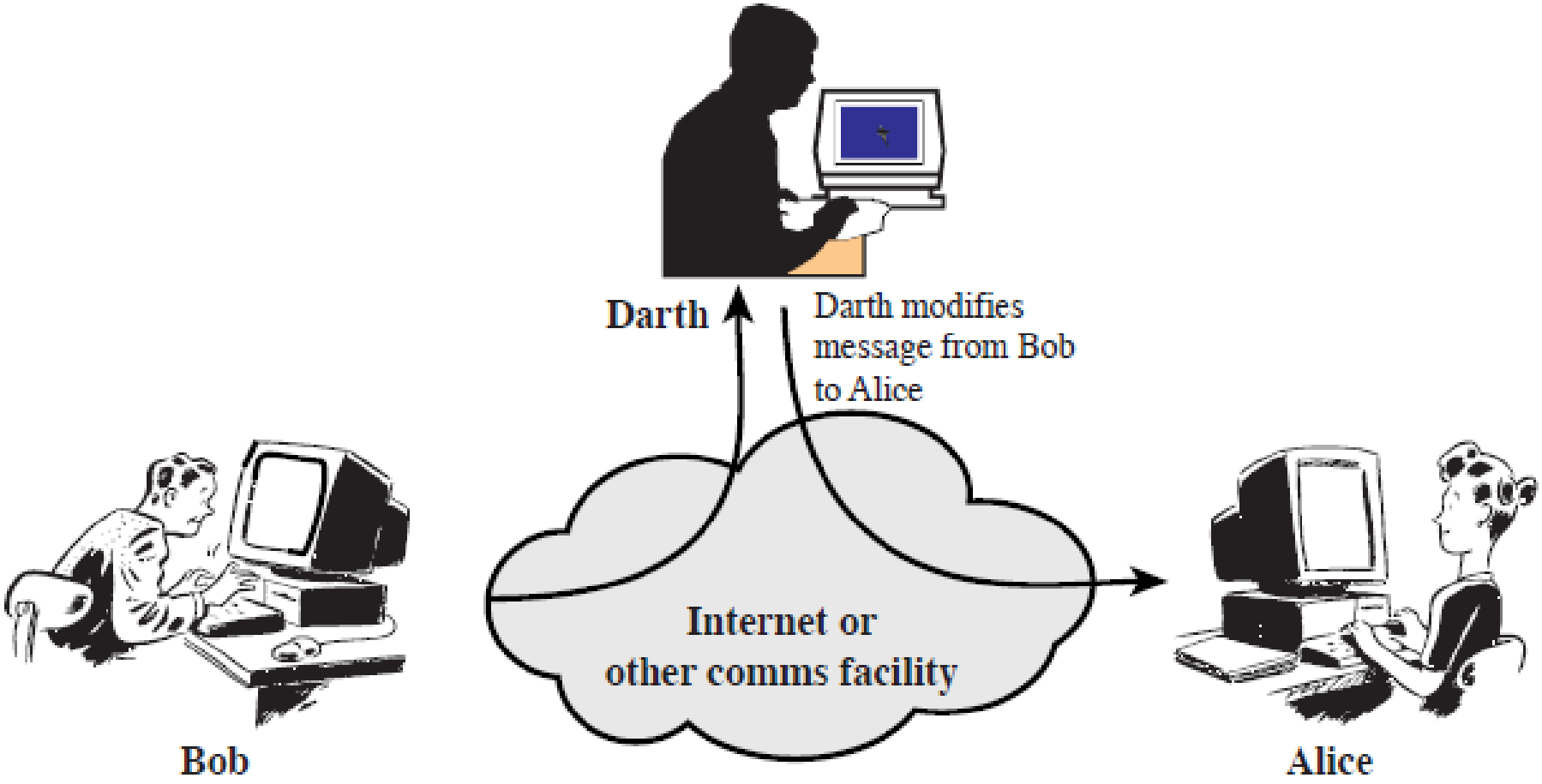
(a) Masquerade

Active - Replay



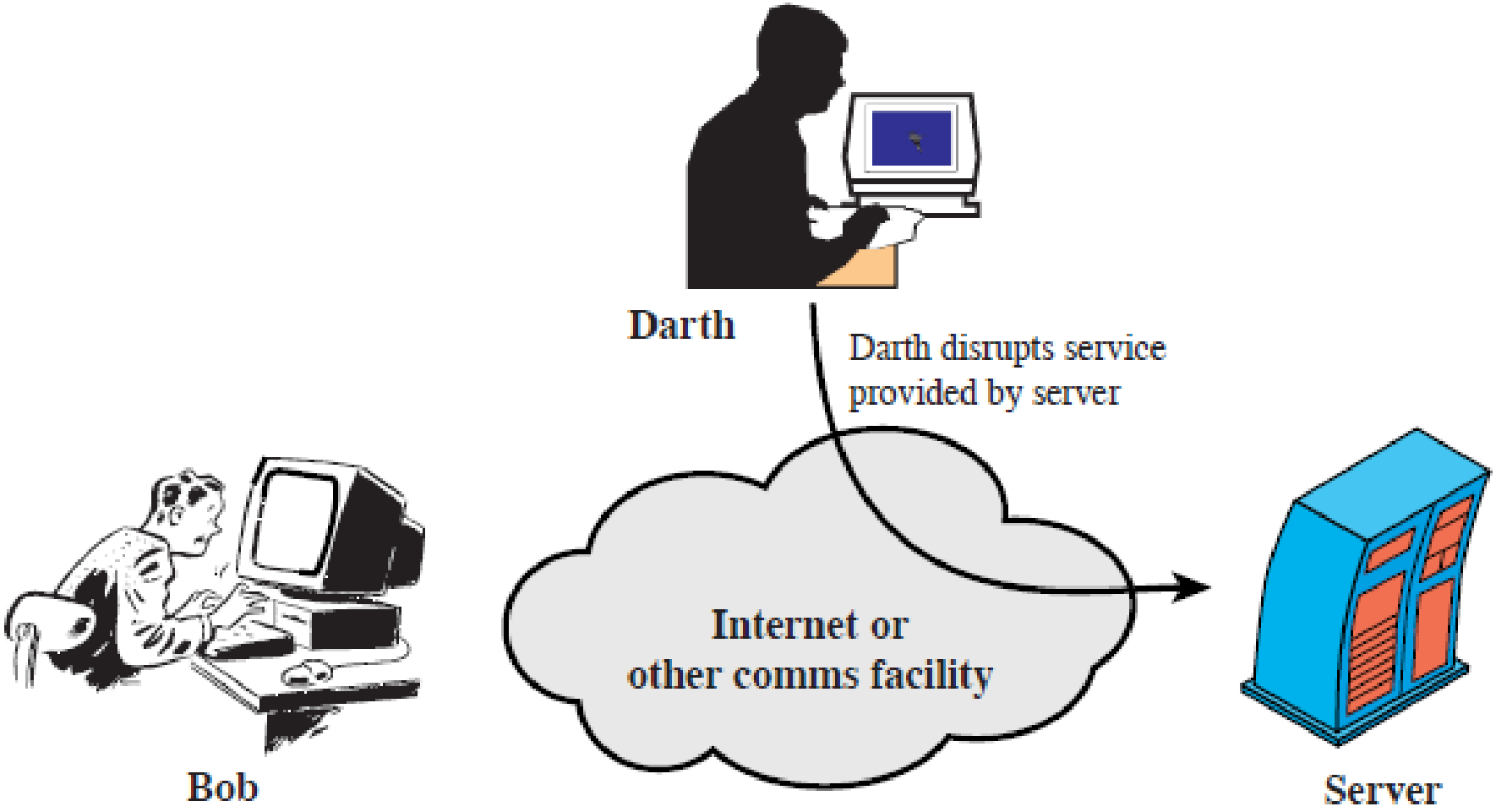
(b) Replay

Active – Intercept & Modify



(c) Modification of messages

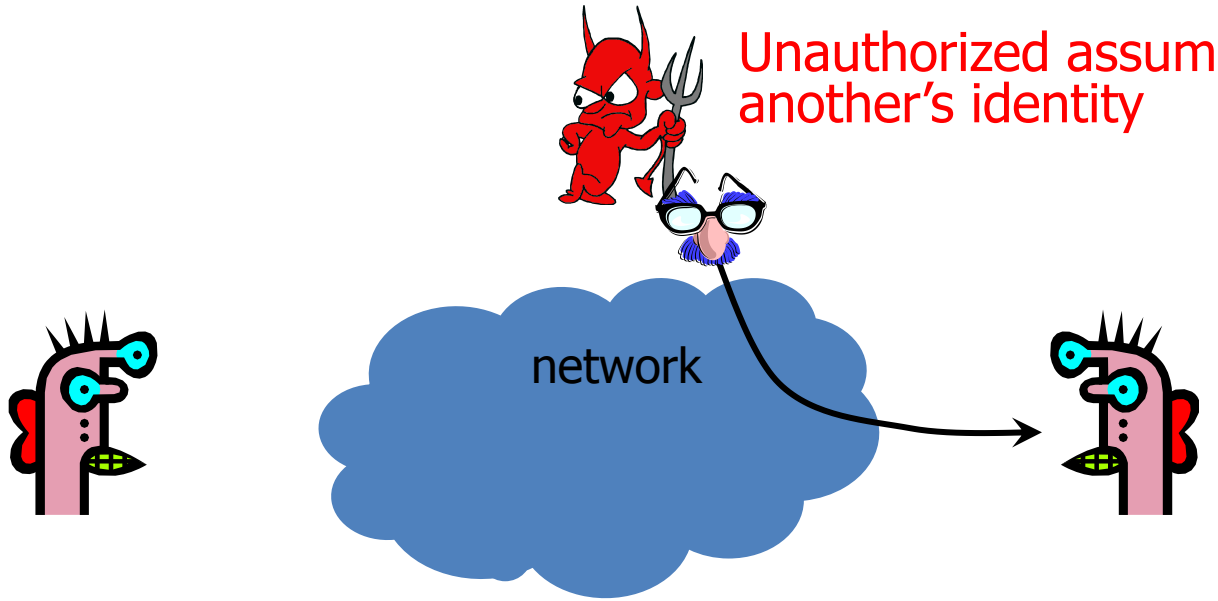
Active - DoS



(d) Denial of service

Attack on Authenticity

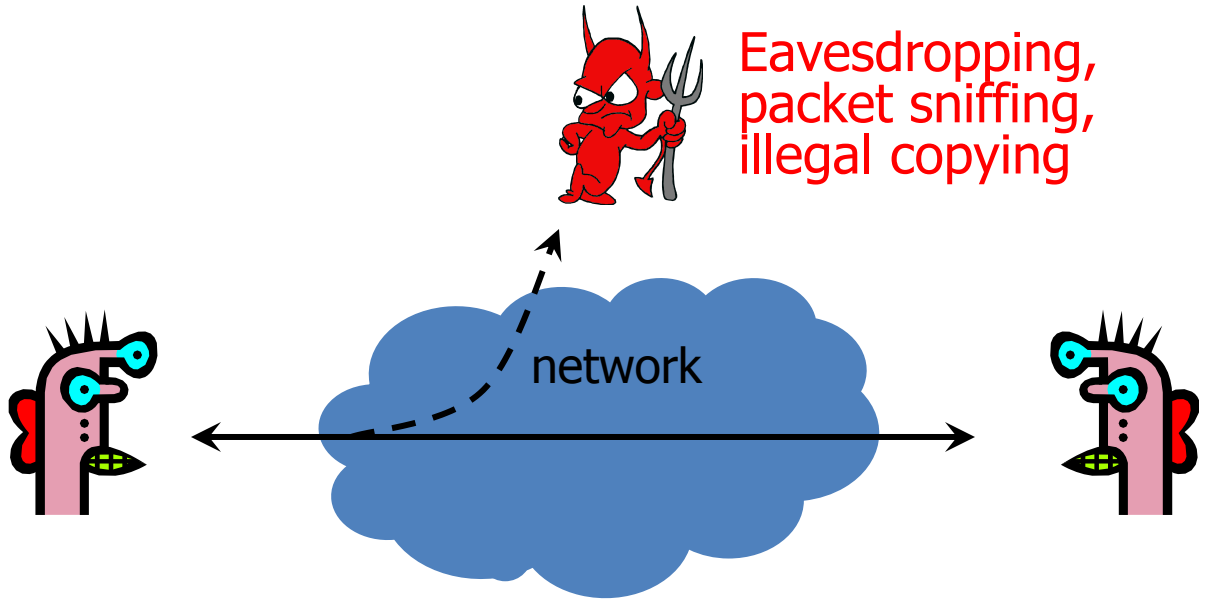
- Authenticity is identification and assurance of origin of information.



In a network scenario.

Attack on Confidentiality

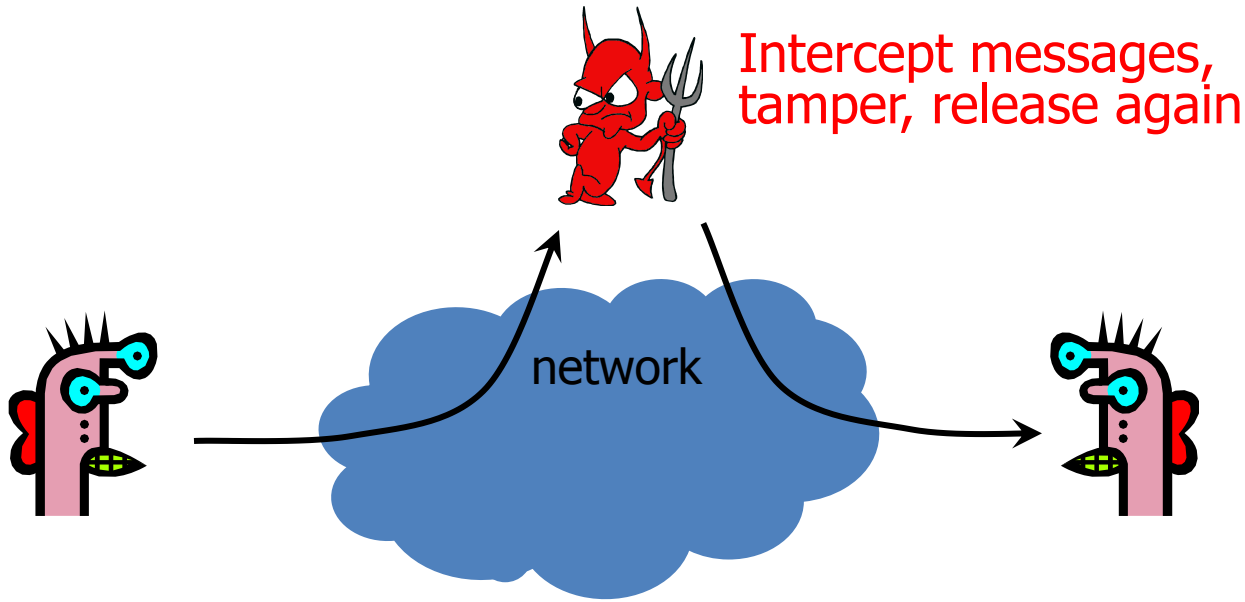
- Confidentiality is concealment of information.



Value of information.

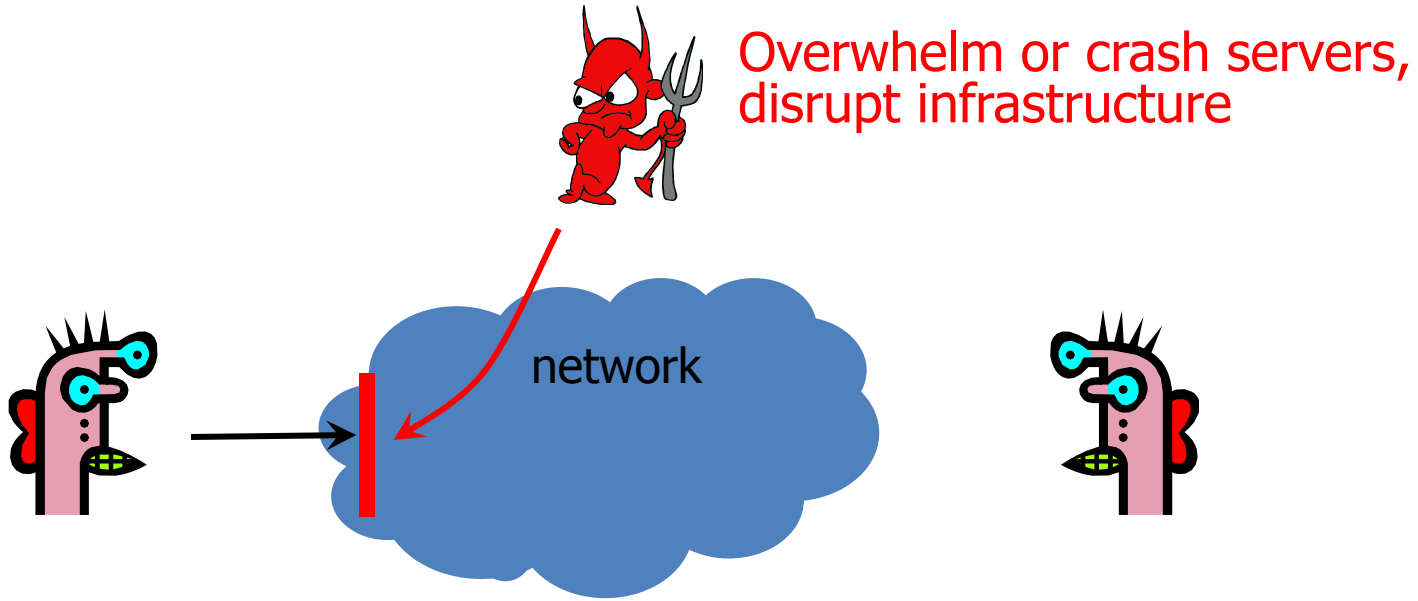
Attack on Integrity

- Integrity is prevention of unauthorized changes.



Attack on Availability

- Availability is ability to use information or resources desired.



Under attack scenario.

Security Attacks

- **Interruption:** This is an attack on
  - availability
- **Interception:** This is an attack on
  - confidentiality
- **Modification:** This is an attack on
  - integrity
- **Fabrication:** This is an attack on
  - authenticity

Sniffing

- It is the easiest attack to launch since all the packets transit through the attacker.

- All the “plaintext” protocols are compromised (the attacker can sniff user and password of many widely used protocol such as telnet, ftp, http).

Data/Packet Injection

- Possibility to add packets to an already established connection.
- The attacker can modify the sequence numbers and keep the connection synchronized while injecting packets.
- If the MITM attack is a “proxy attack” it is even easier to inject (there are two distinct connections).

Command Injection

- Useful in scenarios where a one-time authentication is used.
- In such scenarios, sniffing the password is useless, but hijacking an already authenticated session is critical.
- Injection of commands to the server.
- Emulation of fake replies to the client.

Malicious Code Injection

- Insertion of malicious code into web pages or mail (javascript, trojans, virus).
- Modification on the fly of binary files during the download phase (virus, backdoor).

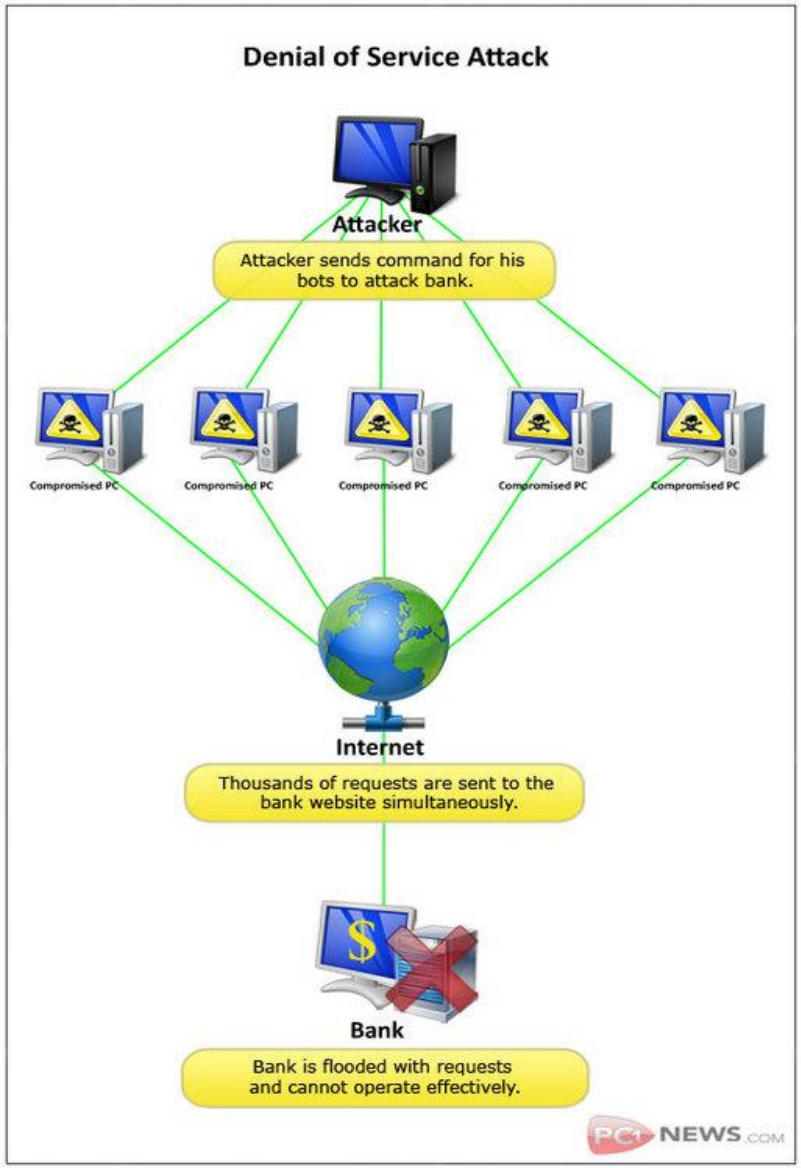
Parameters Substitution

- Parameters exchanged by server and client can be substituted in the beginning of a connection (algorithms to be used later).
- Example: the attacker can force the client to initialize a SSH1 connection instead of SSH2.
  - The server replies in this way:
    - SSH-1.99 -- the server supports ssh1 and ssh2
    - SSH-1.51 -- the server supports ONLY ssh1
  - The attacker makes a filter to replace “1.99” with “1.51”

DDoS Attack

Flooding

- Attacker sends an overwhelming number of messages to your machine; great congestion.
- The congestion may occur in the path before your machine.
- Messages from legitimate users are crowded out.
- Usually called a Denial of Service (DoS) attack, because that's the effect.
- Usually involves a large number of machines, hence Distributed Denial of Service (DDoS) attack.



As of 2013, the PCeU is being merged into the National Cyber Crime Unit, part of the new National Crime Agency.

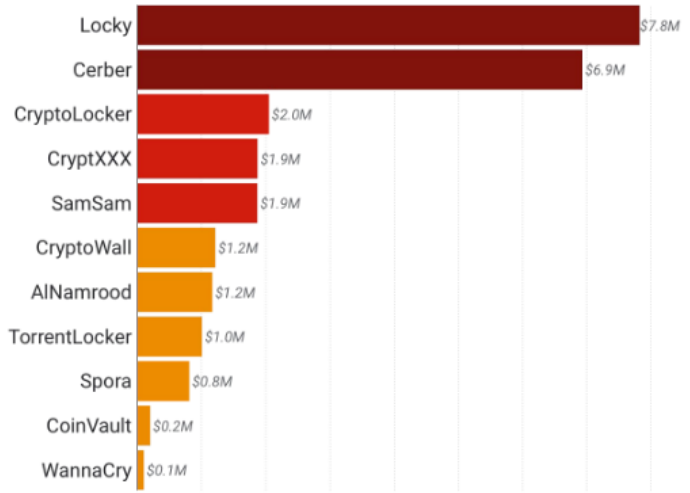
Ransomware

- **Ukash Ransomware -** pretends alert from PCeU.
- Asking you to pay a fine of 100£ in the form of a Ukash or PaySafecard code.
- Also has the ability to access your installed webcam.

- Ignore any such alert and remove this Trojan ransomware.
- Under no circumstance should you send any money to PCeU cyber criminals as this could lead to identity theft.

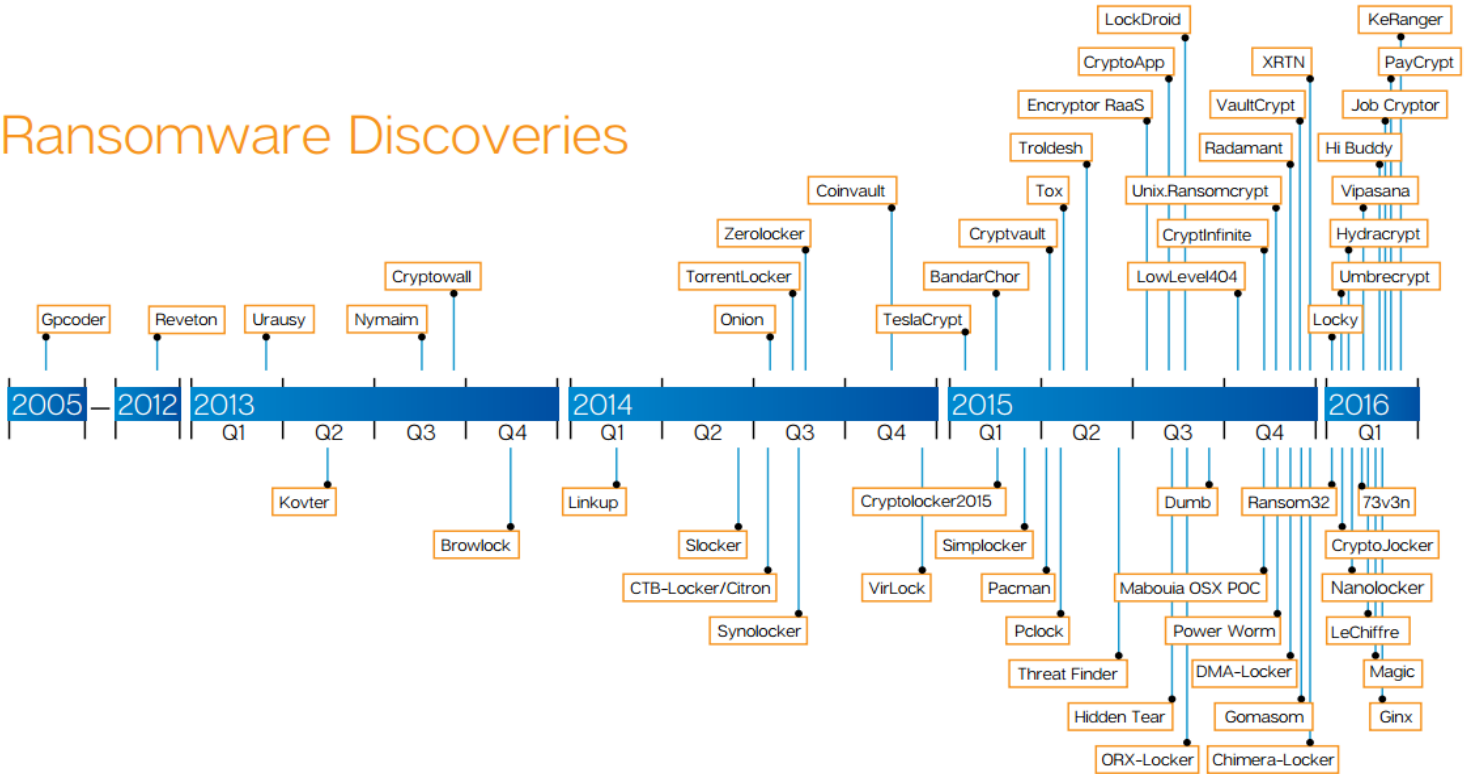
- Remove Trojan:
  - System restore
  - Malwarebytes anti-malware
  - HitmanPro (cloud anti-malware)
  - Kaspersky rescue disk

Ransomware



The ecosystem is dominated by a few kingpins

Ransomware Discoveries

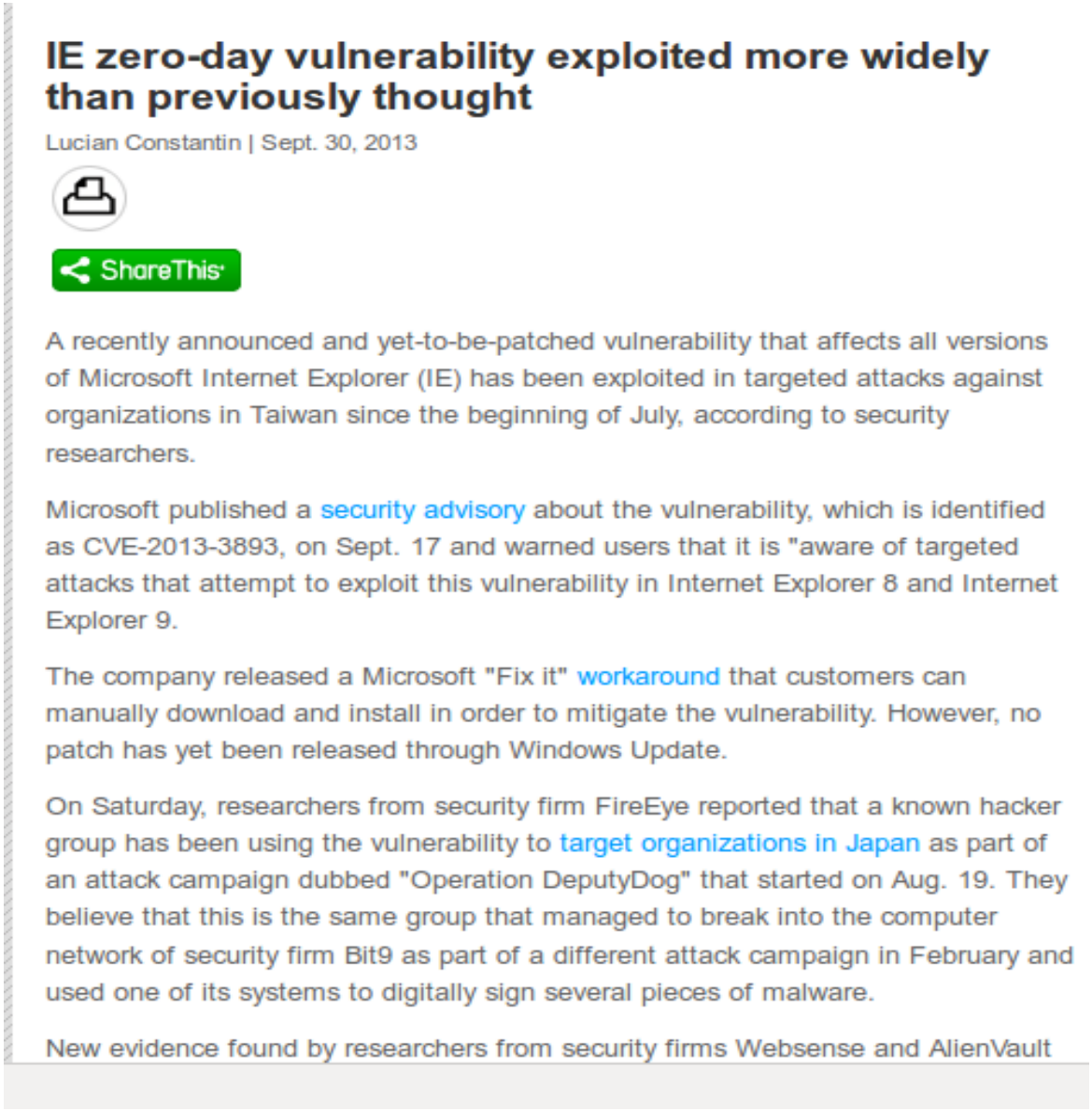


0-day (Zero Day) Vulnerabilities

It is an unknown exploit that exposes a vulnerability in software or hardware and can create complicated problems well before anyone realizes something is wrong.

In fact, a zero-day exploit leaves NO opportunity for detection ... at first.

The term ‘zero-day’ refers to an unknown vulnerability that the developer is newly aware of, and thus an official patch or update to fix the issue has not been released.



IE zero-day vulnerability exploited more widely than previously thought

Lucian Constantin | Sept. 30, 2013

ShareThis

A recently announced and yet-to-be-patched vulnerability that affects all versions of Microsoft Internet Explorer (IE) has been exploited in targeted attacks against organizations in Taiwan since the beginning of July, according to security researchers.

Microsoft published a security advisory about the vulnerability, which is identified as CVE-2013-3893, on Sept. 17 and warned users that it is "aware of targeted attacks that attempt to exploit this vulnerability in Internet Explorer 8 and Internet Explorer 9.

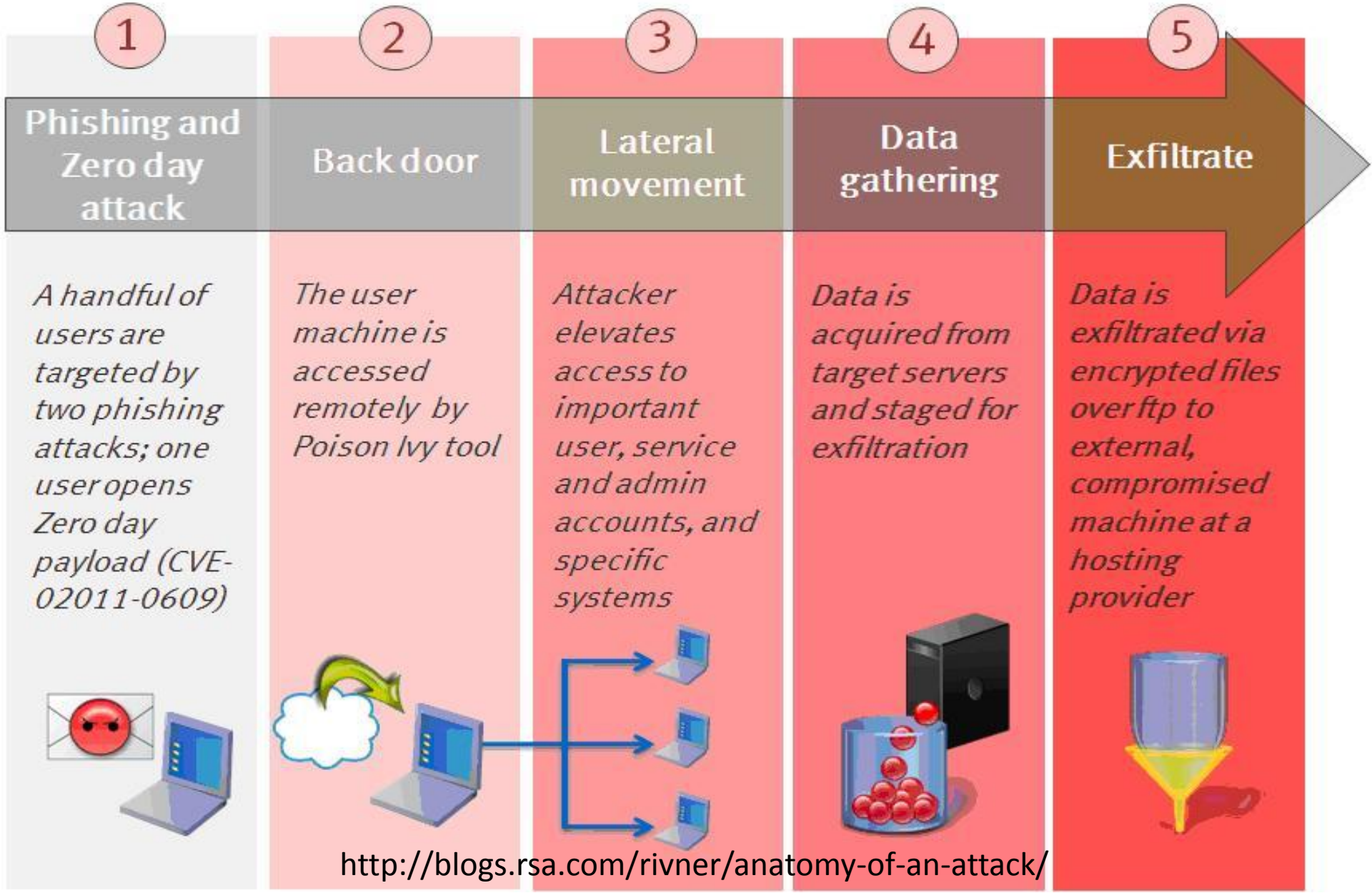
The company released a Microsoft "Fix it" workaround that customers can manually download and install in order to mitigate the vulnerability. However, no patch has yet been released through Windows Update.

On Saturday, researchers from security firm FireEye reported that a known hacker group has been using the vulnerability to target organizations in Japan as part of an attack campaign dubbed "Operation DeputyDog" that started on Aug. 19. They believe that this is the same group that managed to break into the computer network of security firm Bit9 as part of a different attack campaign in February and used one of its systems to digitally sign several pieces of malware.

New evidence found by researchers from security firms Websense and AlienVault

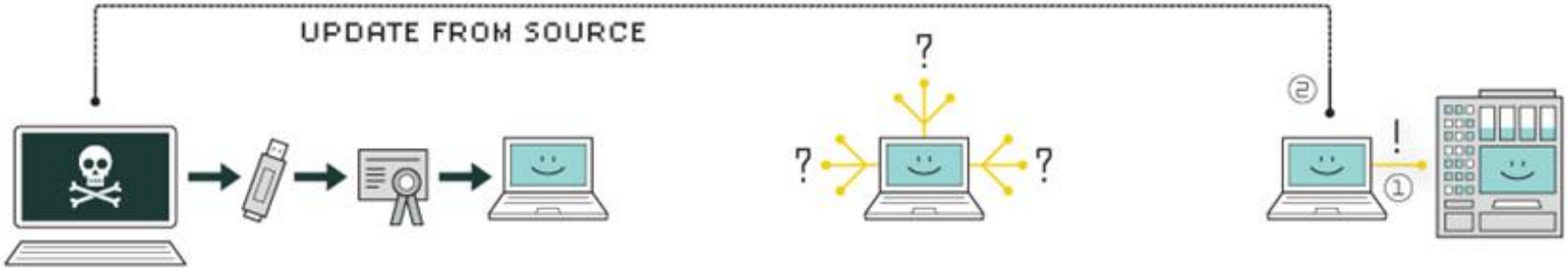
http://www.computerworld.com.sg/tech/internet/ie-zero-day-vulnerability-exploited-more-widely-than-previously-thought/

Advanced Persistent Threat (APT)



http://blogs.rsa.com/rivner/anatomy-of-an-attack/

Stuxnet



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

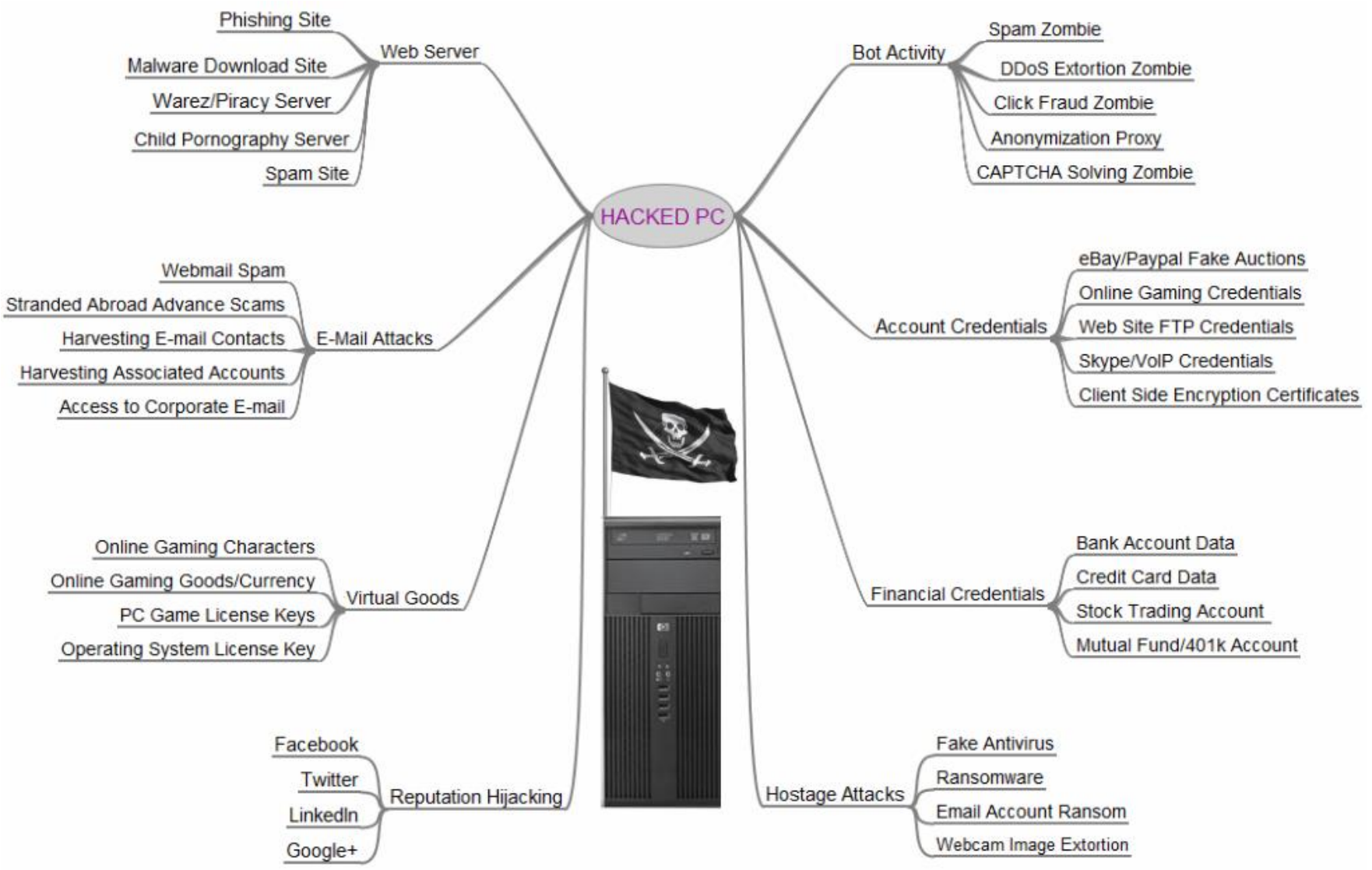
3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Why Should I Care?



http://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/

Human Factors/Usable Security

- *User: “How can I secure my computer against all cyber attacks?”*
- *Security person: “Easy. Disconnect it from the internet, turn it off and put it back in the box. And who said you could unpack it?”*
- Usable security also covers the design, development, configuration and maintenance of the tools and systems the business runs on.

Cont.

- Poor usability often = poor security
- *It's worth bearing in mind that usability doesn’t depend on security (you can easily make a product very simple to use, and also very insecure), but security often does depend on usability.*
- If a product has to be used in a particular way in order to be secure - but people cannot easily use it that way - the product is not secure in any meaningful sense.

Human Factors/Usable Security

- **Usability**
  - assesses how easy user interfaces are to use.
  - also refers to methods for improving ease-of-use during design process.

- Usability is defined by **5 quality components**:
- **Learnability**:
  - How easy is it for users to accomplish basic tasks the first time they encounter the design?
- **Efficiency**:
  - Once users have learned the design, how quickly can they perform tasks?
- **Memorability**:
  - When users return to the design after a period of not using it, how easily can they re-establish proficiency?
- **Errors**:
  - How many errors do users make, how severe are these errors, and how easily can they recover from the errors?
- **Satisfaction**:
  - How pleasant is it to use the design?

Cont.

- Utility = whether it provides the **features you need**.
- Usability = how **easy & pleasant** these features are to use.
- **Useful = usability + utility**.

- e.g., software based on password policy, authentication policy, web login page, mobile phone login access, etc.