Significance of Cyber Security & Human Rights

Dr. Ch. Rupa
Professor,
Dept. of CSE
V. R. Siddhartha Engineering College (A)
Vijayawada

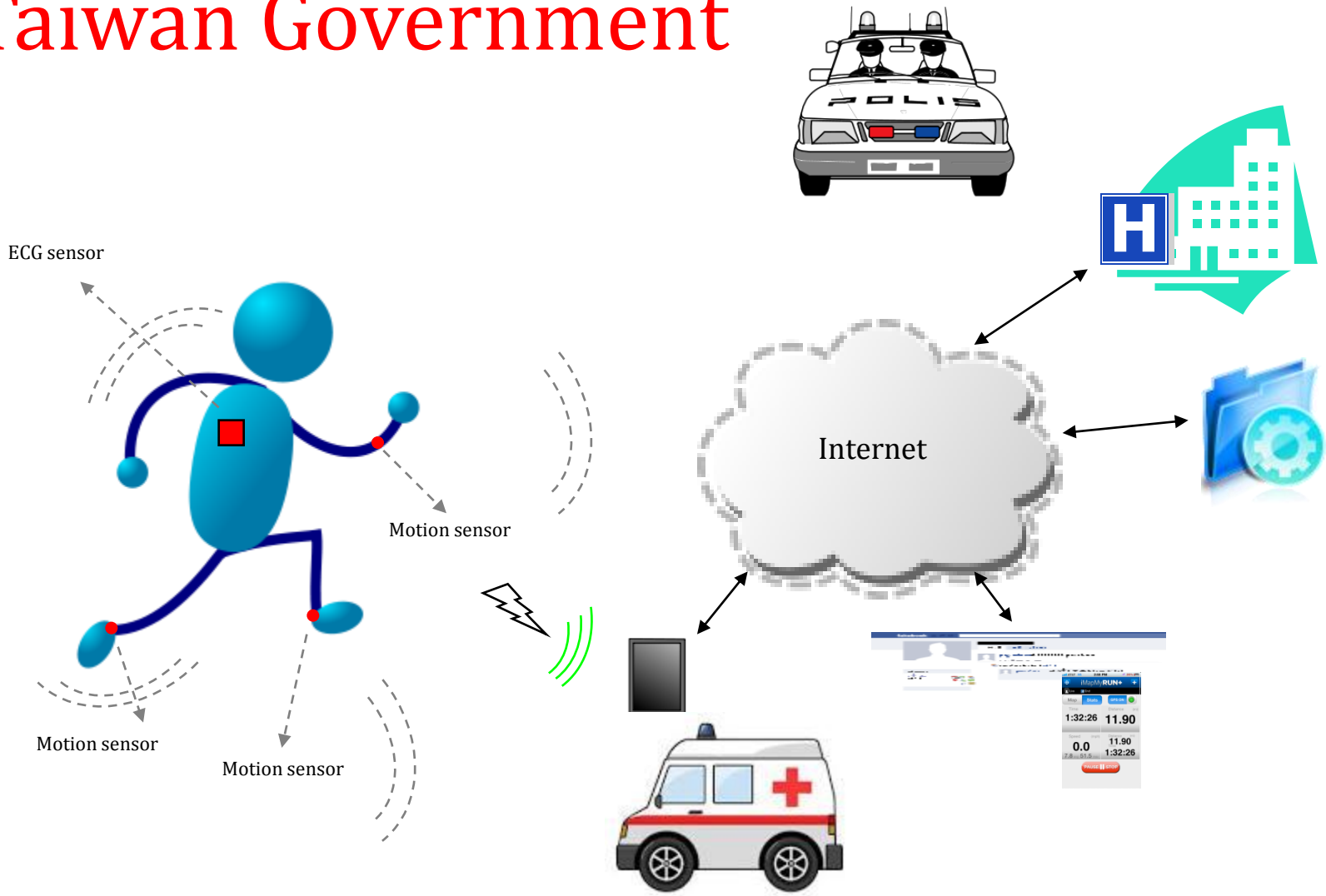
Samsung Admits Its Smart TV Is Spying On You

December 2012: a vulnerability in Samsung Smart TVs that allows an intruder to take control of the devices that are connected to the same network.

November 2013: LG's Smart TVs are sending personal information back to the company's servers about what channels you watch and viewing habits.

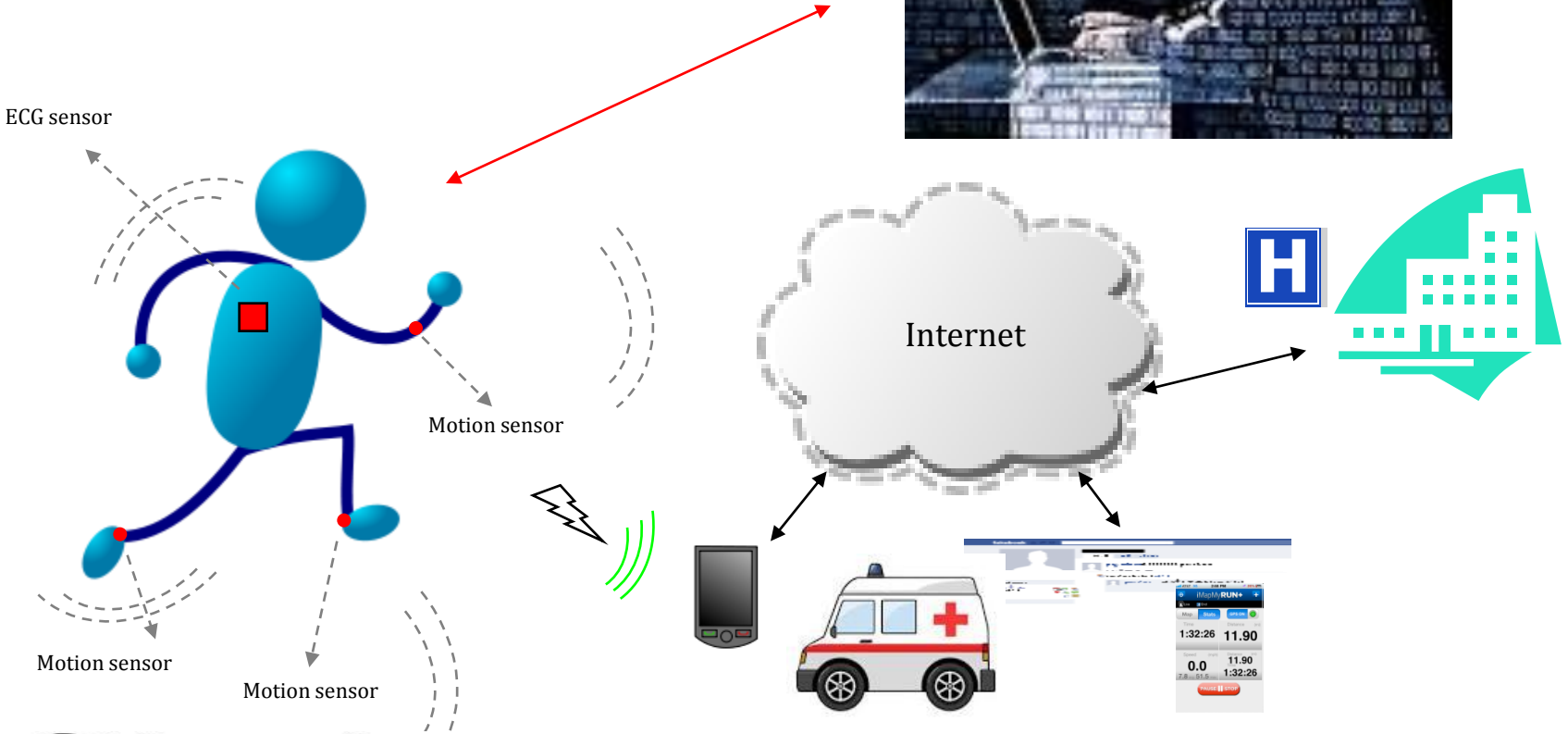
July 2013: Another vulnerability allowed hackers to remotely crash Samsung Smart TV without doing much efforts

Taiwan Government



People Connecting to Things

What happens?



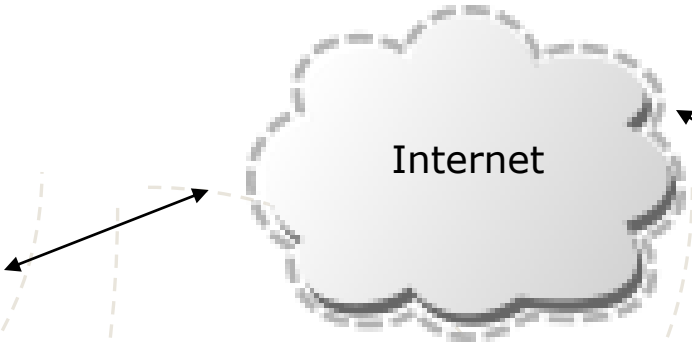
The Telegraph

Home Video News World Sport Finance Comment Culture Travel Life Wome
Politics | Election 2015 | Investigations | Obits | Education | Science | Earth | Weather | Healt
Science News | Dinosaurs | Space | Night Sky | Evolution | Picture Galleries | Science Video

HOME » NEWS » SCIENCE » SCIENCE NEWS

Terrorists could hack pacemakers like in Homeland, say security experts

Smart Fridge



For The First Time, Hackers Have Used A Refrigerator To Attack Businesses

JULIE BORT | JAN 17, 2014, 12.06 AM

Issues

Consequences...

- Loss of Individual Privacy
- Authentication
- Loss of Confidentiality
- Loss of Credibility
- Data manipulation (Denmark Example)
- Data Protection (Not possible to tamper with)
- Data Maintenance (Update/ Modify when needed, like change of address in AADHAR card etc)

Problems that can lead to...

- Blackmailing
- Trolling
- DOS and DDOS Attacks
- Replay attack (Creating Delay)
- Intersection
- Fabrication
- Modification
- Interception

Concepts

Basic Concepts of Security

- Confidentiality : limiting information access and disclosure to authorized users -- "the right people" -- and preventing access by or disclosure to unauthorized ones -- "the wrong people".

- Authentication : process by which a system/person verifies the identity of a User who wants access to some resource.

  Access Control is normally based on the identity of the User who requests access to a resource

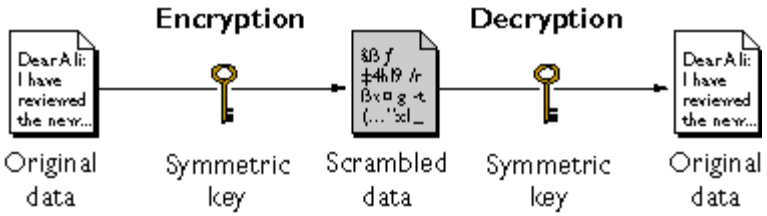
Methods

- Symmetric Key Encryption
- Asymmetric /Public Key Encryption

Symmetric Key Encryption

- It is a form of computerized cryptography using a single encryption key to guise an electronic message.
- Its data conversion uses a mathematical algorithm along with a secret key, which results in the inability to make sense out of a message.
- Symmetric encryption is a two-way algorithm because the mathematical algorithm is reversed when decrypting the message along with using the same secret key.

Symmetric Key Encryption Cont'd...



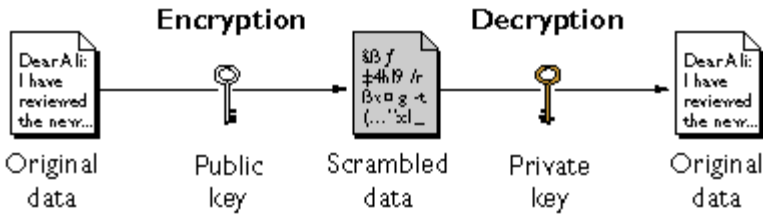
Asymmetric/ Public Key Encryption

- Public-key encryption involves a pair of keys-a public key and a private key-associated with an entity that needs to authenticate its identity electronically or to sign or encrypt data.

- Each public key is published, and the corresponding private key is kept secret.

- Data encrypted with your public key can be decrypted only with your private key.

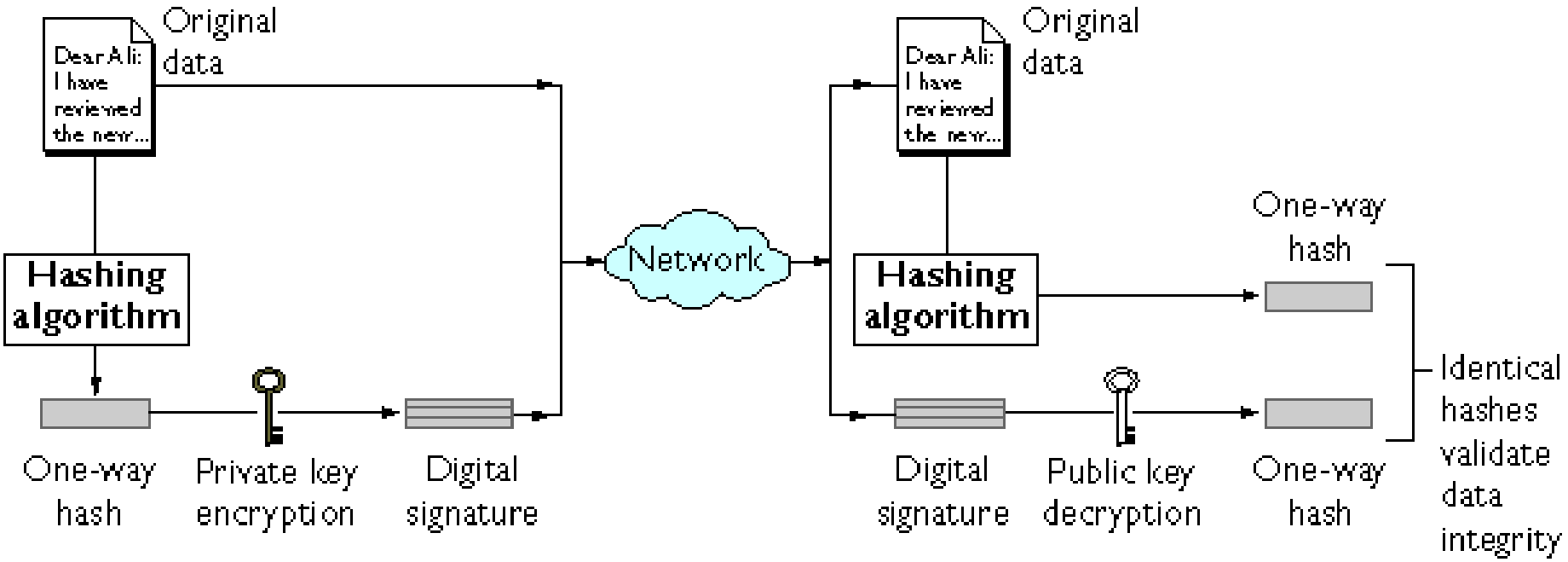
Asymmetric/ Public Key Encryption - Cont'd...



Some Definitions

- Hashing: Extracting the sensitive part of a message of fixed size such that any change in the massage reflects in hashing of that message
- Message Digest: Hashed Message
- Digital Signature: is encrypted message digest.
- It is basically a way to ensure that an electronic document (e-mail, spreadsheet, text file, etc.) is **authentic.**

Authentication Using Digital Signature



Authentication Methods

- Passwords
- Biometrics
  - Finger
  - Hand
  - Face
  - Iris
  - CAPTCHAs (Limited Applicability)

Digital Certification

- The Digital Certificate is a common credential that provides a means to verify identity of an entity.
- A trusted organization assigns a certificate to an individual or an entity that associates a public key with the individual.
- The person or entity to whom a certificate is issued is called the subject of that certificate.

Digital Certification

- The trusted organization that issues the certificate is a Certification Authority (CA) and is known as the certificate's issuer.

- A trustworthy CA will only issue a certificate after verifying the identity of the certificate's subject.

SSL

- Secure Sockets Layer (SSL) is a standard protocol used for the secure transmission of documents over a network.
- It creates a secure link between a Web server and browser to ensure private and integral data transmission.
- SSL uses Transport Control Protocol (TCP) for communication.

SSL

- Secure Sockets Layer (SSL) is a standard protocol used for the secure transmission of documents over a network.
- It creates a secure link between a Web server and browser to ensure private and integral data transmission.
- SSL uses Transport Control Protocol (TCP) for communication.

Cyberspace – Human Rights

- Virtual World of Internet
- Laws governing this area

IT ACT 2000

- The **Information Technology Act, 2000** (also known as **ITA-2000**, or the **IT Act**) .
- It is an Act of the Indian Parliament (No 21 of 2000) notified on 17 October 2000.
- It is the primary law in India dealing with cybercrime and electronic commerce.

What does IT Act 2000 legislation deals with?

- Legal Recognition of Electronic Documents
- Legal Recognition of Digital Signatures
- Offenses and Contraventions
- Justice Dispensation Systems for cyber crimes.

IT Act 2008

- IT (Amendments) Act 2008, it effected from 2009.
- It introduced section 66A, 69.

Notable features of the ITAA 2008 are:

1. Focusing on data privacy
2. Focusing on Information Security
3. Defining cyber café
4. Making digital signature technology neutral
5. Defining reasonable security practices to be followed by corporate