NETWORK
SECURITY

PTIIK - 2012

Networking … at a glance

Discrete Mathematics

Advance Networking

Operating Systems

Network Analysis

Computer Networks

Multimedia Networking

Network Security

Network Programming

Distributed Systems

System Administrations

Course Design

- Classes
  - 2 Credits
- Exercises (assistant required)
  - 1 Credits
- Evaluation
  - 2 Structured Task (20 %)
  - 1 Midterm Test (40 %)
  - 1 Final Test (40 %)

References

- Douligeris, Christos : “Network Security : *Current Status and Features Directions*” , John Wiley & Sons , 2007
- Kizza, Joseph Migga: “Computer Network Security” , Springer, 2005
- Canavan, John E : “Fundamentals of Network Security” , Artech House , 2001
- Cole, Eric : “Network Security Bible” , John Wiley & Sons , 2005

References

- Skoudis, Edward: “Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses Second Edition” , Prentice Hall , 2006
- Mogollon, Manuel: “Cryptography and Security Services : Mechanisms and Applications” , Cybertech , 2007
- Rhee, Man Young: “Internet Security, Cryptographic Principles, Algorithms and Protocols” , John Wiley & Sons , 2003

Course Content

- 01 Introduction
  - 1.1 Some Terminology
  - 1.2 Network Security Attacks
  - 1.3 Sources of Security Threats
  - 1.4 Security Threat
    - 1.4.1 Motives
    - 1.4.2 Management
    - 1.4.3 Correlation
    - 1.4.4 Awareness

0 Current State

Control systems

automobile

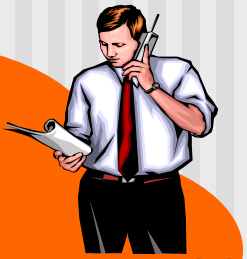
Home appliances

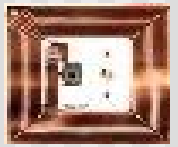
Smart Cards

Cellular phone

Power supply

The Internet

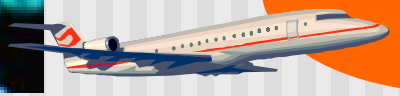




RFID

Our activities

Traffic control



Aviation services

Medical services

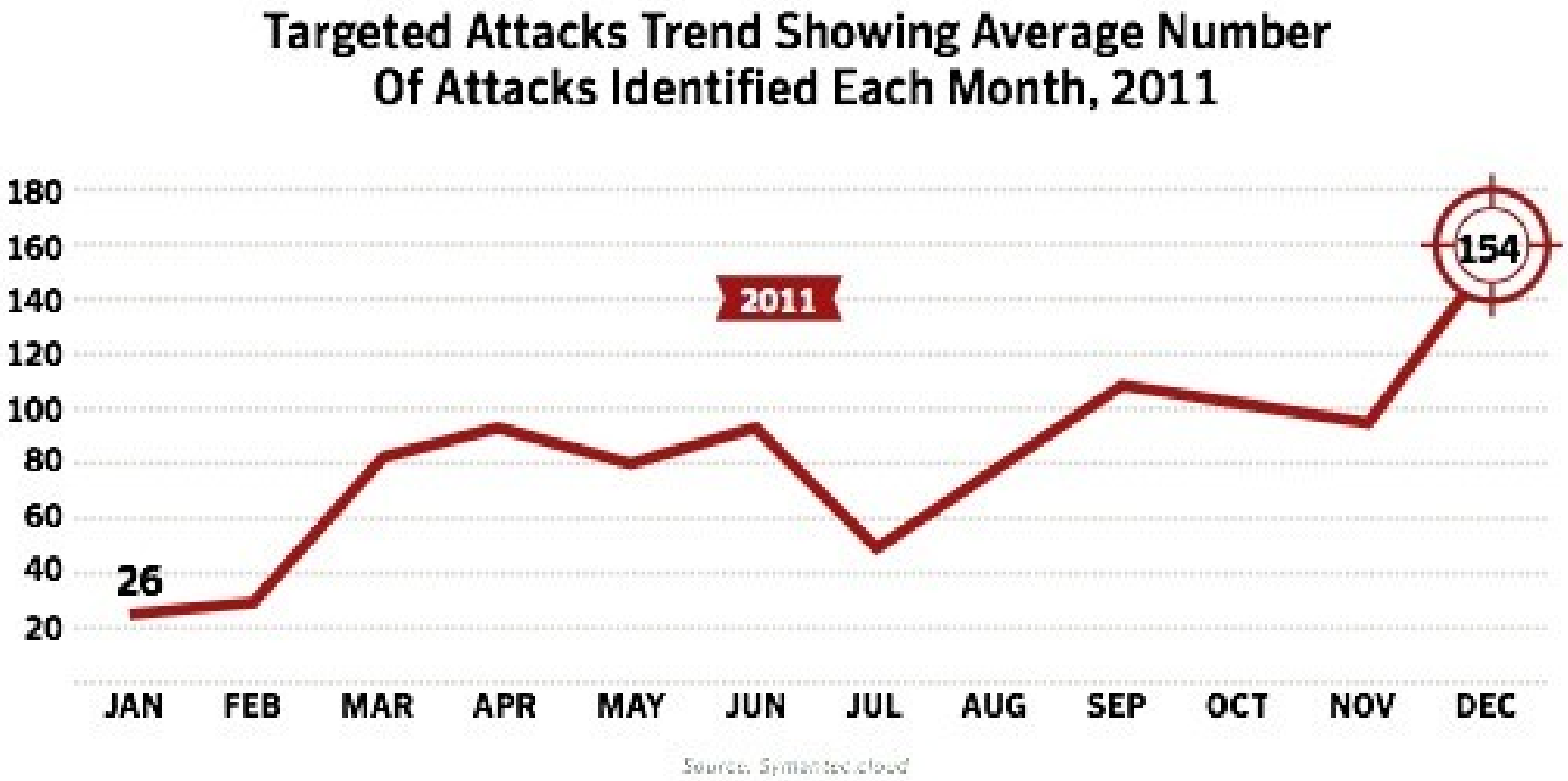
Financial services

Online banking

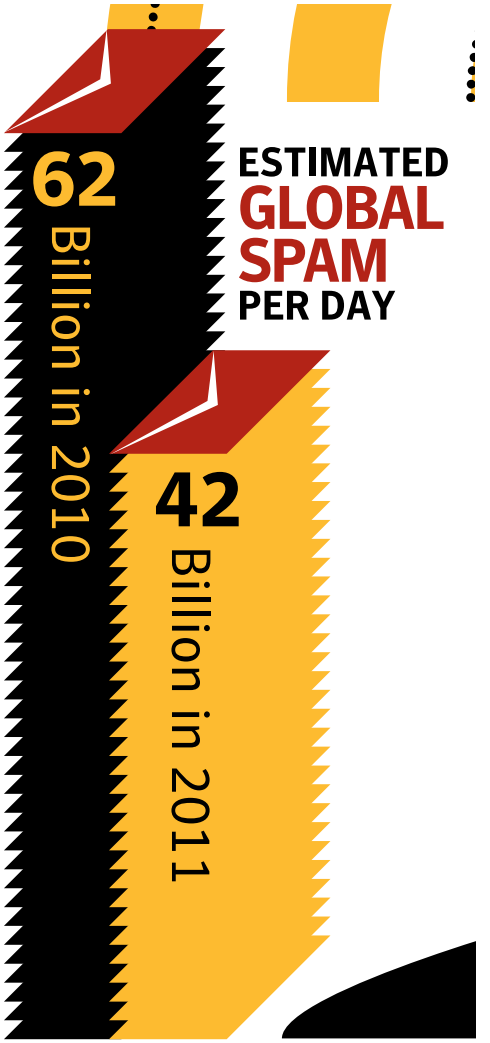
Reservation & ticketing

ATM

0 Current State



0 Current State



0 Current State

Figure 7

Top-Ten Sectors By Number Of Data Breaches, 2011

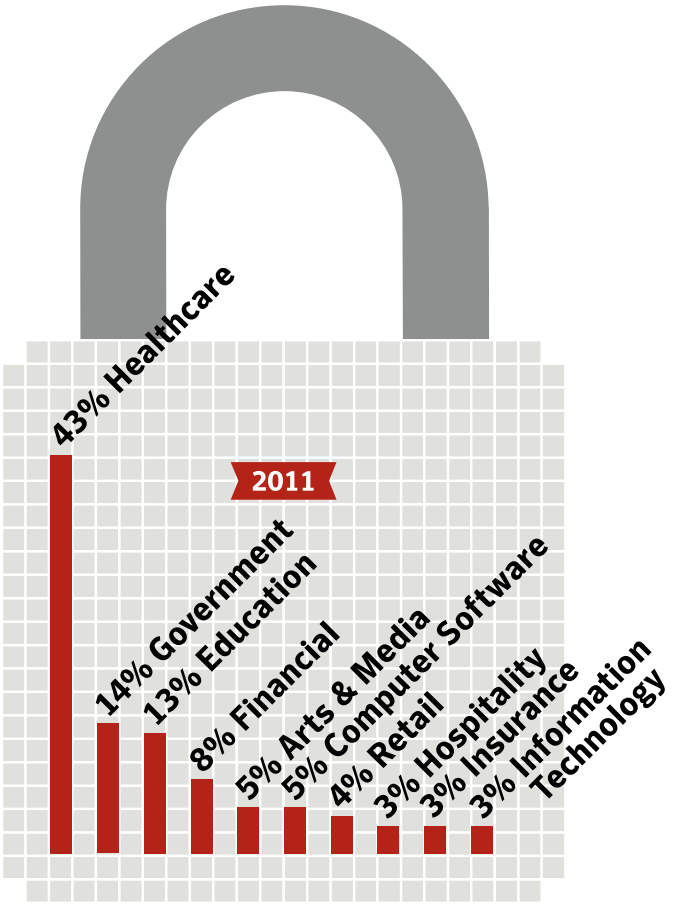
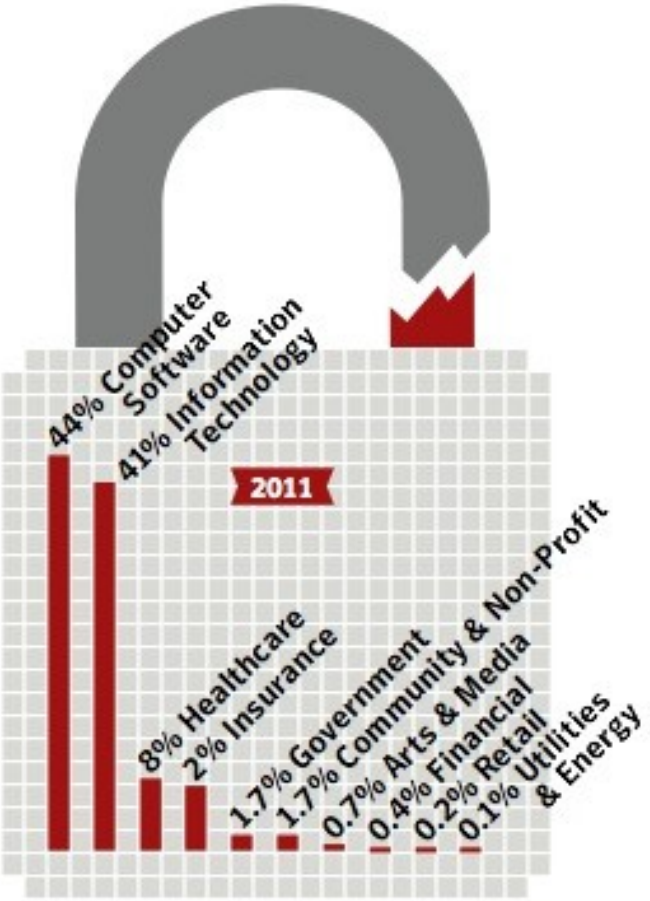


Figure 8

Top-Ten Sectors By Number Of Identities Exposed, 2011

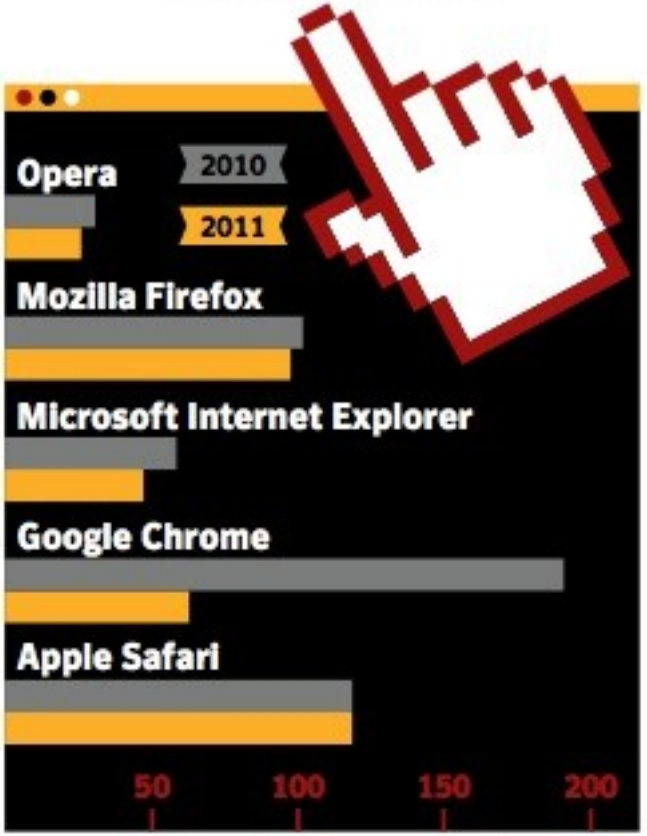


Source: Symantec

0 Current State

Figure 19

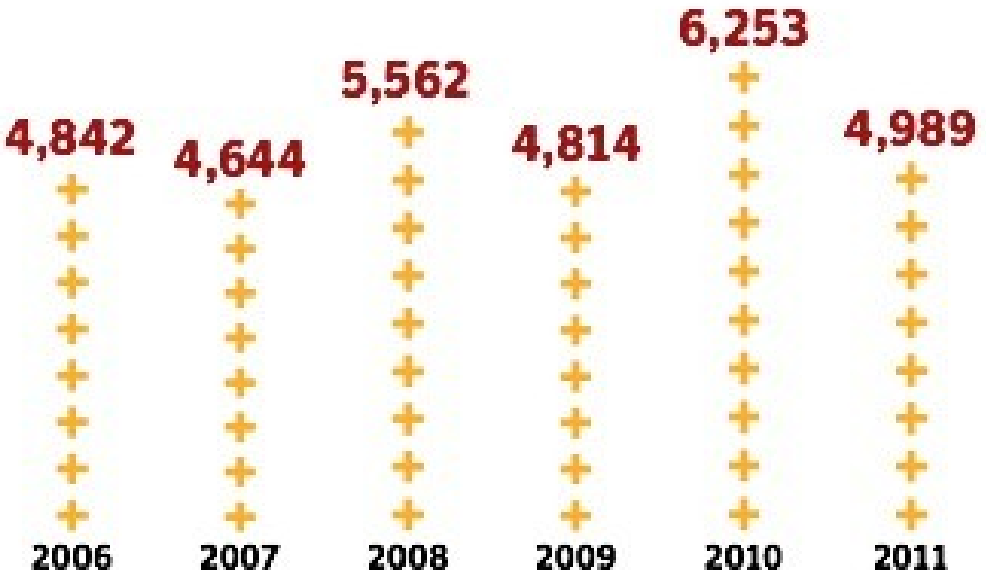
Browser Vulnerabilities In 2010 And 2011



Source: Symantec

Figure 18

Total Number Of Vulnerabilities Identified, 2006-2011



Source: Symantec

0 Current State

- Top-5 Most Infected Websites
  - Blogs and Web communications.
  - Hosting/Personal hosted sites.
  - Business/Economy.
  - Shopping.
  - Education and Reference.

Current State

- Web based attacks increased by 36% with over 4,500 new attacks each day.
- 403 million new variants of malware were created in 2011, a 41% increase of 2010.
- SPAM volumes dropped by 13% in 2011 over rates in 2010.
- 39% of malware attacks via email used a link to a web page.
- Mobile vulnerabilities continued to rise, with 315 discovered in 2011.

1.1 Some Terminology

- Definition of *network security* can be constructed by defining its two components, *security* and *networks.*
- **Security** can be defined as follows:
  - A situation with no risk, with no sense of threat.
  - The prevention of risk or threat.
  - The assurance of a sense of confidence and certainty.

1.1 Some Terminology

- **Security**, is described through the accomplishment of some basic security properties, namely *confidentiality*, *integrity*, and *availability* of information.
  - **Confidentiality** is the property of *protecting information from* all non-intended or *unauthorized users.*
  - **Integrity** is the property of *protecting* the content of *information from alteration* by unauthorized users.

1.1 Some Terminology

- **Availability** is the property of *protecting information from non authorized temporary or permanent withholding* of information.
- Other basic properties of security is *authentication* and *nonrepudiation*.
  - **Authentication** is divided into *peer-entity* authentication and *data origin* authentication.
    - ***peer-entity*** authentication is the property of *ensuring the identity* of an entity (or subject), i.e. human, machine, or software.
    - **data-origin** authentication is the property of *ensuring the source* of information.

1.1 Some Terminology

- **Nonrepudiation** is the property of *ensuring* that *principals* that have committed to an action *cannot deny* that *commitment* at a latter time.
- In practical approach, **security** *involves* the *protection of information assets*
  - **Assets** may be
    - *physical* (computers, network infrastructure elements, buildings hosting equipment),
    - *data* (electronic files, databases), or
    - *software* (application software, configuration files).

1.1 Some Terminology

- The protection of assets can be achieved through several *security mechanisms*, that is, aimed at the *prevention*, *detection*, or *recovery* of assets from security *threats* and *vulnerabilities.*
  - **Threat** is *any event that may harm* an asset. When it is realized, system is under *attack*.
  - **Vulnerability** is *any characteristic in a system which makes an asset more vulnerable to threats*.

1.1 Some Terminology

- *The combination of threats, vulnerabilities, and assets provides a quantified and/or qualified measure*, that known as **risk**.

- **Network security** can be considered through the achievement of two security goals:
  - ***computer system security***, to protect information assets; and
  - ***communication security***, to protect information during its transmission

  against *unauthorized* or *malicious use* as well as *disclosure*, *modification*, or *destruction*.

1.2 Network Security Attack

- Some basic network security attacks :
  - ***Eavesdropping***, an unauthorized interception of network communication and the disclosure of the exchanged information by:
    - ***Sniffing***, in the network layer, or
    - ***Wiretapping***, in physical layer.
  - ***Logon Abuse***, bypass the authentication and access control mechanisms and allow a user to obtain access with more privileges than authorized.

1.2 Network Security Attack

- ***Spoofing***, is the act of a subject asserting an identity that the subject has no right to use. For example: IP Spoofing.
- ***Intrusion Attacks***, focus on unauthorized users gaining access to a vulnerable system through the network.
- ***Hijacking Attacks***, attempts to gain unauthorized access to a system by using a legitimate entity's existing connection.

1.2 Network Security Attack

- ***Denial-of-Service (DoS) Attacks***, attempts to exhaust the network or server resources in order to render it useless for legitimate hosts and users. Some well known DoS attacks:
  - ***SYN Attack*.** In a SYN attack, the attacker exploits the inability of a server process to handle unfinished connection requests.
  - ***Ping of Death*.** An early DoS attack in which an attacker sends a ping request that is larger than 64Kb, which is the maximum allowed size for the IP, causing the system to crash or restart.

1.2 Network Security Attack

- ***Application-Level Attacks.*** These attacks are concerned with the exploitation of weaknesses in the application layer and really focus on intrusion attacks in most cases. Examples of these attacks include:
  - *malicious software attacks (viruses, Trojans, etc.),*
  - *Web server attacks,*
  - *remote command execution,*
  - *Structured Query Language (SQL) injection*, and
  - *cross-site scripting (XSS)*.

1.3 Sources of Security Threats

- The security threat to computer systems springs from a number of factors that include:
  - weaknesses in the network infrastructure and communication protocols,
  - the growth of the hacker community,
  - the vulnerability in operating system protocols,
  - the insider effect resulting from workers who steal and sell data of the company,
  - social engineering,
  - physical theft, etc.

1.3 Sources of Security Threats

1.3.1 Design Philosophy

- The growth of the Internet and cyberspace in general was based on an ***open architecture work in progress*** philosophy.
- ***The lack*** of a ***comprehensive blueprint*** and the ***demand-driven design*** and ***development of protocols*** are causing the ever present weak points and loopholes in the underlying computer network infrastructure and protocols.

1.3 Sources of Security Threats

1.3.2 Infrastructure and Protocol Weaknesses

- As packets are *di-assembled*, *transmitted*, and *re-assembled*, then there are areas where, through *port scans*, determined users have managed to *intrude*, *penetrate*, *fool*, and *intercept* the packets.
- Initial communication process, called *three way handshake* that involves a *port number*, suffers from *a half-open* socket problem as it leave an open port for further communication.

1.3 Sources of Security Threats

- *Packet transmissions* between network elements can be *intercepted* and their *contents altered* such as in *initial sequence number attack.*
- Infrastructure vulnerability attacks also include *session attacks*, *packet sniffing*, *buffer overflow*, and *session hijacking*.

1.3.3 Rapid Growth of Cyberspace

- As more and more people enjoyed the potential of the Internet, Such individuals have posed a potential risk to the information content of the Internet and such a security threat has to be dealt with.

1.3 Sources of Security Threats

1.3.4 The Growth of the Hacker Community

- The number one contributor to the security threat of computer and telecommunication networks is the growth of the hacker community.

1.3.5 Operating Systems Vulnerability

- the greatest security threat to global computer systems is the area of software errors especially network operating systems errors.

1.3 Sources of Security Threats

1.3.6 The Invisible – Insider Effect

- 75 percent of the IT managers indicated they believed authorized users and employees represent a threat to the security of their systems.
- Its found that in small companies, 32 percent of the worst incidents were caused by insiders, and that number jumps to 48 percent in large companies.

1.3 Sources of Security Threats

1.3.7 Social Engineering

- Social engineering consists of an array of methods an intruder such as a hacker, both from within or outside the organization, can use to gain system authorization through masquerading as an authorized user of the network.

1.3.8 Physical Theft

- Thousands of company executive laptops and PDA disappear every year with years of company secrets

1.4 Security Threats

1.4.1 Motives

- **Terrorism**, electronic terrorism is used to attack military installations, banking, and many other targets of interest.
- **Espionage**, gaining access to highly classified commercial information.
- **Vendetta** or revenge.
- **Notoriety**, proving hacking competencies.
- **Greed**, Many intruders into company systems do so to gain financially from their acts.

1.4 Security Threats

1.4.2 Management

- Security threat management is a technique used to monitor security systems in real-time to review reports from the monitoring sensors such as the intrusion detection systems, firewall, and other scanning sensors.
- It is important for the response team to study the risks as sensor data come in and decide which threat to deal with first.
- Forensic analysis is done after a threat has been identified and contained.

1.4 Security Threats

1.4.3 Correlation

- Security teams have to reduce *the turnaround time*, the time between the start of an incident and the receipt of the first reports of the incident.
- Threat correlation, therefore, *is the technique designed to reduce the turnaround time by monitoring all network sensor data*.
- In fact threat correlation helps in:
  - reducing false positives,
  - reducing false negatives,
  - verifying sensor performance and availability.

1.4 Security Threats

- The quality of data coming from the sensor logs depends on several factors including:
  - **Collection**, the collection techniques specify how the data is to be analyzed.
  - **Consolidation**, it is important to find good techniques to filter out relevant data and consolidate sensor data.
  - **Correlation**, a good data mining scheme must be used for appropriate queries.

1.4 Security Threats

1.4.4 Awareness

- Security threat awareness is meant to bring widespread and massive attention of the population to the security threat.