

# *Basics*

# Unintended behavior

Often systems do not behave as we intend.

The unintended behaviors can be traced to:

- environmental disruption,
- operational errors,
- poor design or implementation (bugs),
- deliberate attacks.

These problems mean that systems don't meet their requirements.

# Mitigations and remedies

Some approaches to addressing these problems are:

- environmental disruption:
  - ⇒ stronger interfaces,
  - ⇒ replication,
- operational errors:
  - ⇒ operator tolerance and education,
  - ⇒ better tools,
- poor design or implementation (bugs):
  - ⇒ languages and tools,
  - ⇒ testing,
  - ⇒ verification,
- deliberate attacks:
  - ⇒ lower expectations,
  - ⇒ ???

# Some threats

In order of increasing severity:

- Unintentional blunders.
- Hackers driven by technical challenges.
- Disgruntled employees or customers seeking revenge.
- Criminals interested in personal gain.
- Organized crime interested in hiding something or in financial gain.
- Organized terrorist groups.
- Foreign espionage agents.
- Information-warfare operations intended to disrupt weapons or command structures.

*(Roughly from the Defense Science Board.)*



# Attack goals

The typical goals of attacks are not specific to computer systems:

- Publicity.
- Fraud.
- Theft of intellectual property.
- Destruction (including denial-of-service).
- Invasions of privacy; surveillance.

Intermediate goals (e.g., stealing a password) sometimes are.

# The unchanging nature of security

Security for computer systems is much like security in the rest of the real world.

- It is not black and white.
- It is not about perfect defenses against well-funded, capable, and determined attackers.

## Be Ready for Security



1 Remove EVERYTHING from your pockets before entering. This includes all paper, plastic items, pens and wallets. Place items in the security bin or your carry-on luggage.



2 Take out liquids (in a baggie). Discard all liquids in containers over 3 ounces. The 3-ounce limit does not apply to formula, milk, baby food or medications.



3 Remove all footwear and outerwear.



4 Remove large electronics, including laptops, and place in a separate bin.

Questions? Ask a Transportation Security Officer.



Transportation  
Security  
Administration

Your safety is our priority

[www.tsa.gov](http://www.tsa.gov)

# The unchanging nature of security (cont.)

Security is about

- value
  - sometimes a simple figure,
  - not always easy to calculate,
- locks
  - several kinds,
  - not always cheap,
  - seldom convenient,
  - imperfect.



# The unchanging nature of security (cont.)

Security is also about

- detecting attacks
  - not always possible,
  - not always possible in real time.





# The unchanging nature of security (cont.)

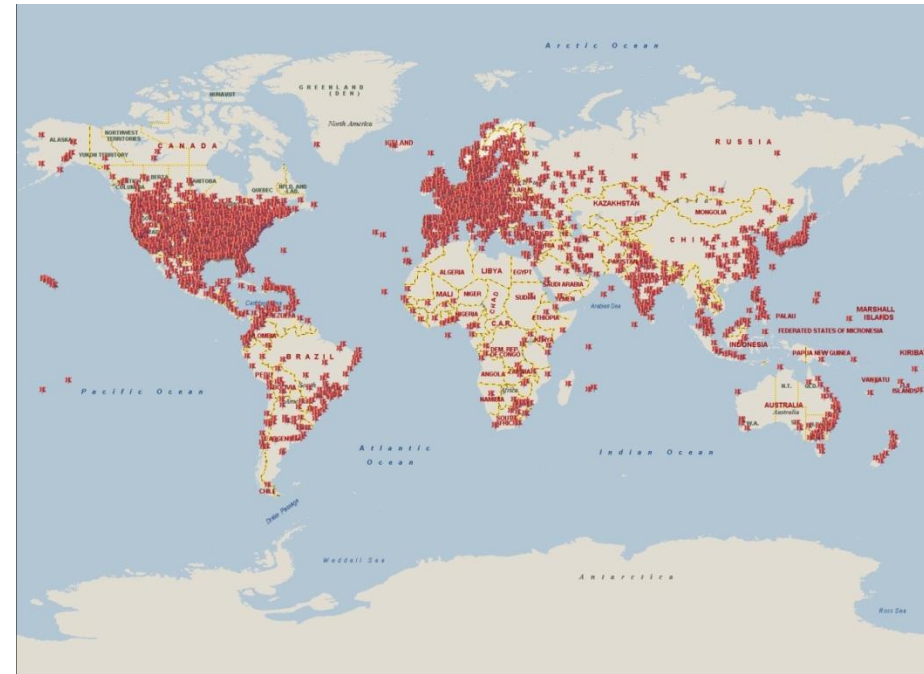
Security is also about

- identifying attackers,
- catching them,
- punishing them.



# Some specific characteristics

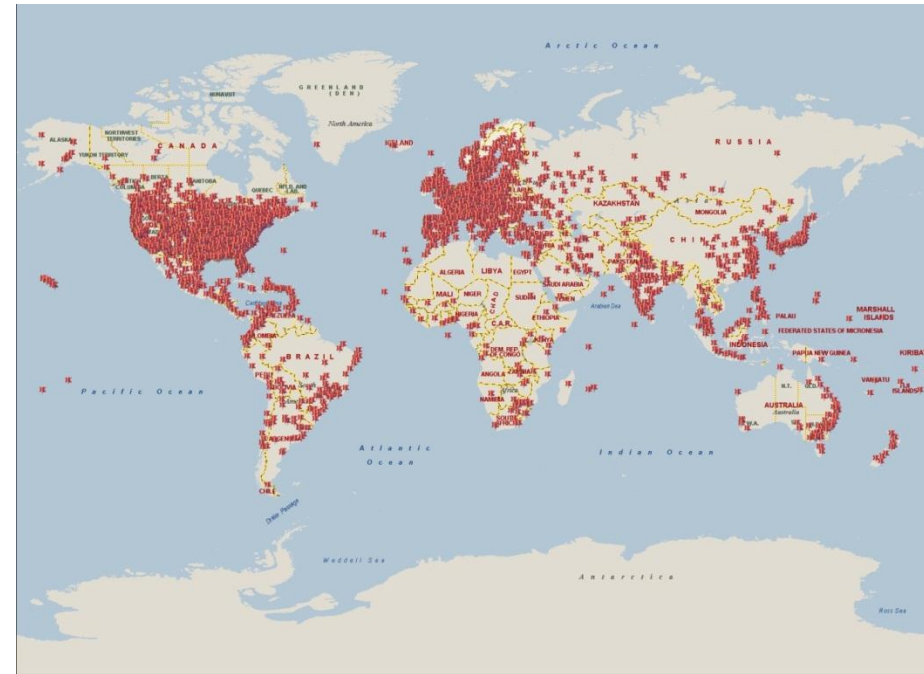
- Attacks can be launched from a distance.
  - Local laws and enforcement often do not suffice.
  - Global cooperation is slow and difficult.



Waledac botnet Source: microsoft.com

# Some specific characteristics (cont.)

- Attacks are often automatic.  
So they can easily be
  - large-scale (against targets everywhere, in various domains),
  - fast,
  - inexpensive.



Waledac botnet Source: microsoft.com

# Some specific characteristics (cont.)

- Attackers can be hard to identify.
- Even attacks can be hard to identify.
- Deterrence is often weak.

September 24, 2010 6:41 AM

**Stuxnet Worm a U.S. Cyber-Attack on Iran Nukes?**

Posted by [Tucker Reals](#)  44 comments

**New Clues Point to Israel as Author of Blockbuster Worm, Or Not**

By [Kim Zetter](#)  October 1, 2010 | 3:45 pm | Categories: [Breaches](#), [Cybersecurity](#)

**Un général israélien revendique la création du virus Stuxnet contre l'Iran**

LEMONDE.FR | 16.02.11 | 16h28

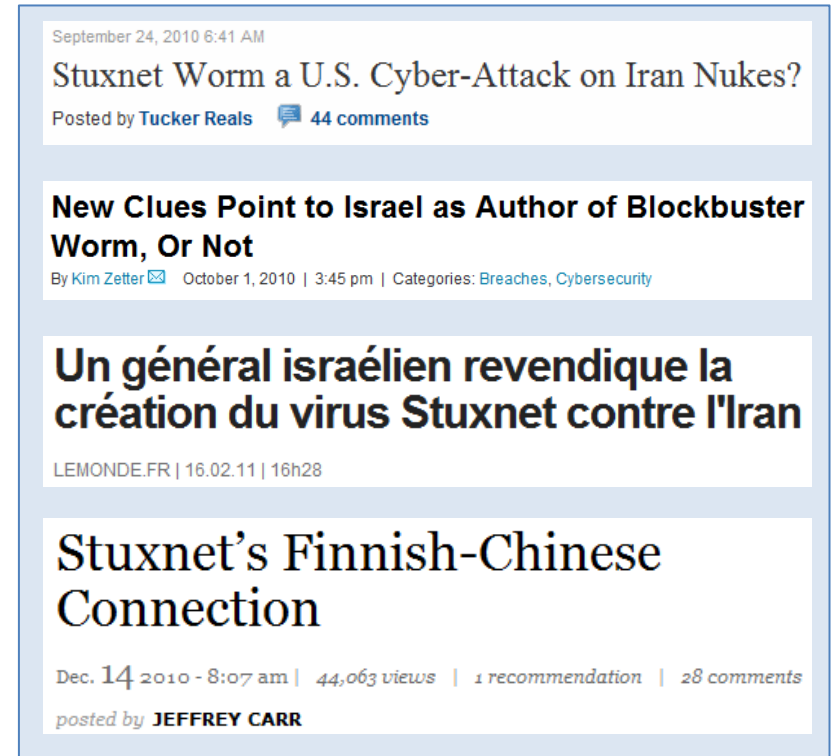
**Stuxnet's Finnish-Chinese Connection**

Dec. 14 2010 - 8:07 am | 44,063 views | 1 recommendation | 28 comments

posted by **JEFFREY CARR**

# Some specific characteristics (cont.)

- Attackers can be hard to identify.
- Even attacks can be hard to identify.
- Deterrence is often weak.



September 24, 2010 6:41 AM  
**Stuxnet Worm a U.S. Cyber-Attack on Iran Nukes?**  
Posted by [Tucker Reals](#) 44 comments

**New Clues Point to Israel as Author of Blockbuster Worm, Or Not**  
By [Kim Zetter](#) | October 1, 2010 | 3:45 pm | Categories: [Breaches](#), [Cybersecurity](#)

**Un général israélien revendique la création du virus Stuxnet contre l'Iran**  
LEMONDE.FR | 16.02.11 | 16h28

**Stuxnet's Finnish-Chinese Connection**  
Dec. 14 2010 - 8:07 am | 44,063 views | 1 recommendation | 28 comments  
posted by [JEFFREY CARR](#)

Some of these characteristics are fairly intrinsic to computing. Others follow from important design choices.

# Vulnerabilities

- ***Vulnerability***: A flaw that can be exploited to breach security.
- ***Attack***: A method of exploiting one or more vulnerabilities.

# The dominant vulnerable systems

Some common system characteristics enable attacks (and aggravate other problems).

- Interaction
  - with an uncertain physical environment (e.g., for a laptop in the enemy's hands),
  - with an uncertain network environment (everything is connected),
  - with an uncertain software environment (e.g., with mobile code in Web pages).

# The dominant vulnerable systems (cont.)

- Distributed administration.
- Diverse operators.
- Importance of time to market (and the market seldom pays for security).
- Open, shared infrastructures (e.g., the Internet).
- Building from commercial, off-the-shelf components.
- Automation, including automated infection!



# The dominant vulnerable systems (cont.)

These characteristics are unlikely to disappear:

- They are the result of fundamental economic or technical trends.
- Many are generally desirable.

# Reading

- Anderson's "Why information security is hard – An economic perspective"

<http://www.cl.cam.ac.uk/~rja14/Papers/econ.pdf>

# Homework 1 (due October 4)

## **Exercise 1:**

Describe an actual security failure in a computer system.

State:

- a) the security property that is violated,
- b) the vulnerability that permits the violation,
- c) the attack that exploits the vulnerability,
- d) if possible, how to address the vulnerability.

You may use whatever sources you like (the Web, newspapers, the scientific literature), but please cite them. A paragraph may suffice; a page should.