Case Study: Stuxnet Malware

Stuxnet 'hit' Iran nuclear plans

The Stuxnet worm might be partly responsible for delays in Iran's nuclear programme, says a former UN nuclear inspections official.

Olli Heinonen, deputy director at the UN's nuclear watchdog until August, said the virus might be behind Iran's problems with uranium enrichment.

Discovered in June, Stuxnet is the first worm to target control systems found in industrial plants.

Analysis carried out by security firm Symantec shows that a Stuxnet-infected controller in an industrial plant would make the devices it was connected to run at very high speeds almost indefinitely.

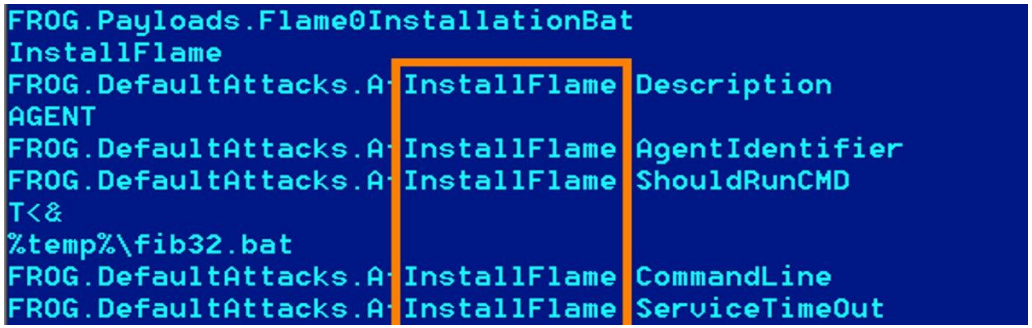
Symantec's research also suggests that Stuxnet was designed to hit motors controlling centrifuges and thus disrupt the creation of uranium fuel pellets.

Figures gathered by security firms show that 60% of all the infections caused by Stuxnet were on machines in Iran.

Case Study: Flame Spyware

Behind the 'Flame' malware spying on Mideast computers (FAQ)

With possible ties to malware targeting Iran, the Flame spying software is seen as the latest cyber espionage attempt from a nation state.



Flame is a sophisticated attack toolkit that leaves a backdoor, or Trojan, on computers and can propagate itself through a local network, like a computer worm does. Kaspersky Lab suspects it may use a critical Windows vulnerability, but that has not been confirmed, according to a Kaspersky blog post. Flame can sniff network traffic, take screenshots, record audio conversations, log keystrokes and gather information about discoverable Bluetooth devices nearby and turn the infected computer into a discoverable Bluetooth device. The attackers can upload additional modules for further functionality. There are about 20 modules that have been discovered and researchers are looking into what they all do. The package of modules comprises nearly 20 megabytes, over 3,000 lines of code, and includes libraries for compression, database manipulation, multiple methods of encryption, and batch scripting.

System Complexity Leads to Insecurity

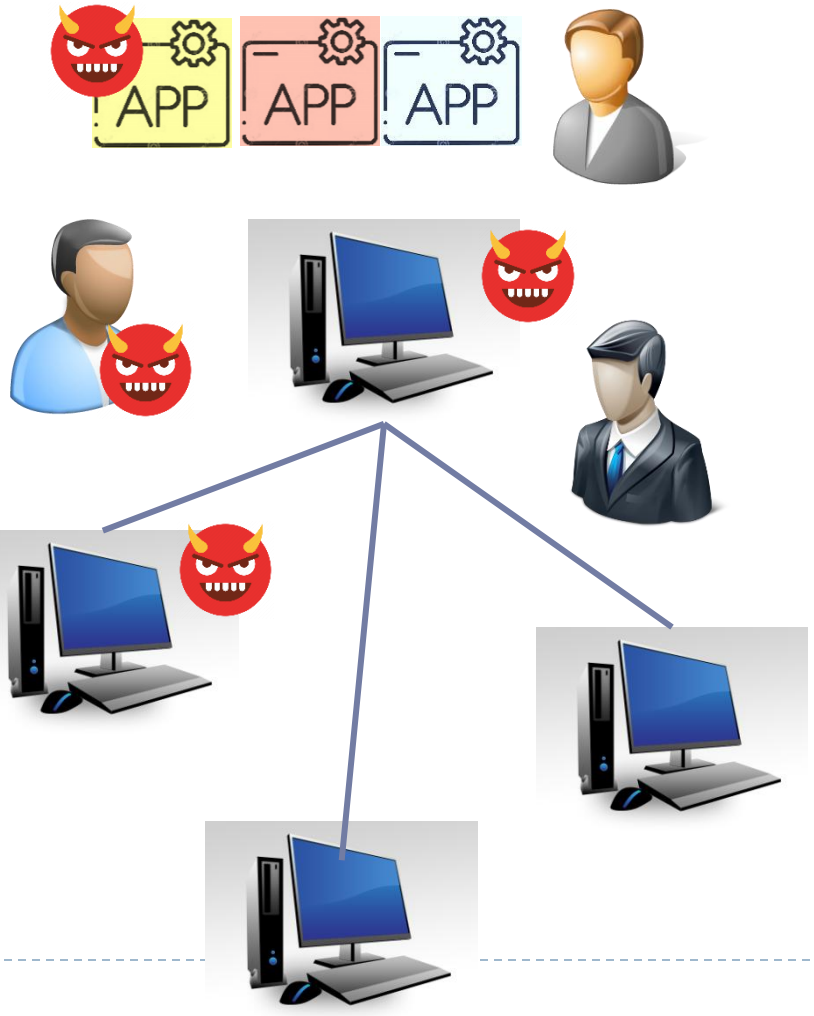
Provide a protected environment for data and their processing

Standalone computer single user monoprogram

- Physical security

Standalone computer single user multiprogram

- Physical security
- Process protection



Standalone computer multiple user

- Physical security
- Process protection
- Data protection
- User authentication

Networked computer

- Physical security
- Process protection
- Data protection
- User authentication
- Communication protection

Human Factors Lead to Insecurity

System Users

- Security features are not used correctly, e.g., misconfiguration.
- Users like convenience and may try to disable some security configurations that are not inconvenient

System Developers

- Security features are not designed correctly; security components are not implemented correctly
- Developers are humans, and humans can make mistakes.

External Parties

- Individual's trust can be manipulated for profit, e.g., social engineering

Basics of Cyber Security

Threat Model

- Trusted Computing Base (TCB)
- Attacker's assumption
- Security properties

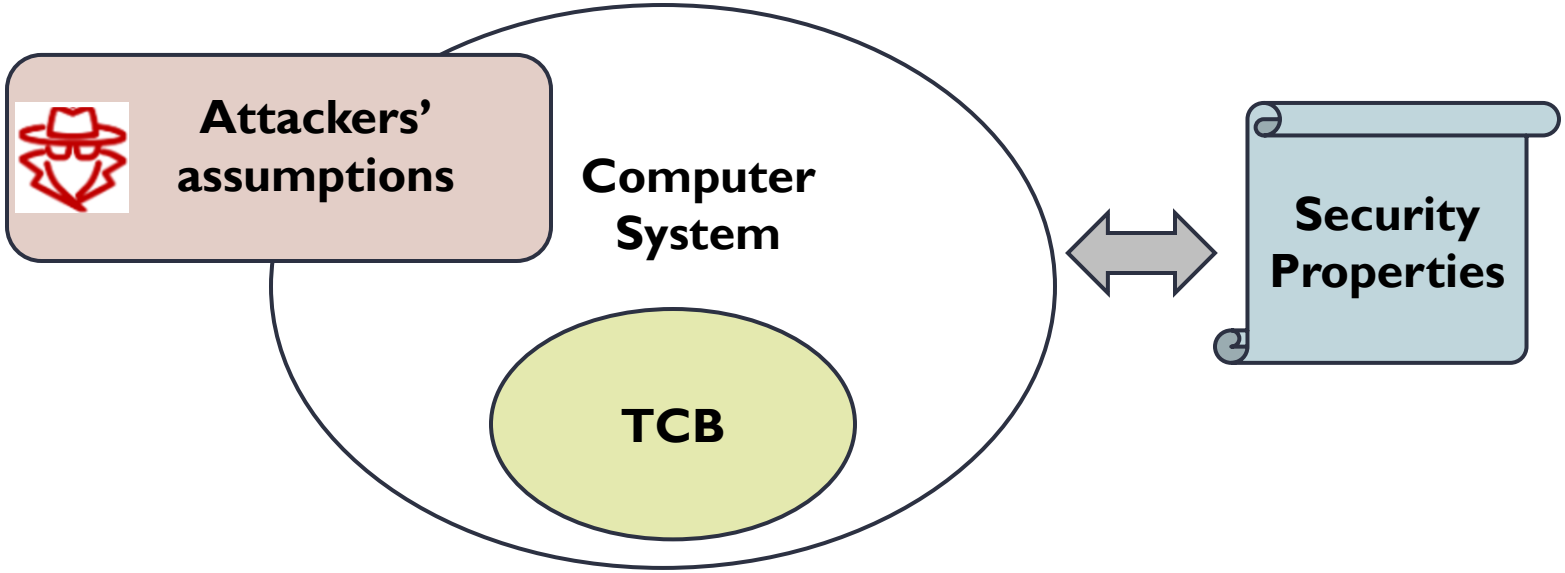
- **Security Strategies**

- **Design Principles of Computer Security**

Threat Model

Describe the adversaries and threats in consideration

- What is trusted and what is not trusted (TCB).
- For the untrusted entities, what resources, capabilities and knowledge they have; what actions they can perform.
- What security properties the system aim to achieve.



Trust

The degree to which an entity is expected to behave:

- What the entity is expected to do:
  - Anti-malware can detect malicious programs;
  - System can prevent illegal account login, etc.
- What the entity is expected not to do:
  - The website will not expose your private data to third parties;
  - An application will not inject virus into your system.

Security cannot be established in a cyber system if no entities are trusted.

It is important to make clear what should be trusted. Otherwise, the designed security solutions may fail in practice.