Helsinki University
of Technology

Utilizing data networks in stealth attacks

professor Hannu H. Kari
Laboratory for Theoretical Computer Science
Department of Computer Science and Engineering
Helsinki University of Technology (HUT), Espoo, Finland
email: Kari [at] tcs [dot] hut [dot] fi

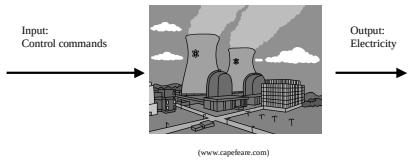
Helsinki University
of Technology

Agenda

- **Introduction**
- **Background**
- **Traditional approach**
- **Definition of stealth attack**
- **Stealth attack against computer networks**
- **Stealth attack methods**
- **Protection methods**
- **Remaining problems**
- **Future studies**
- **Conclusions**

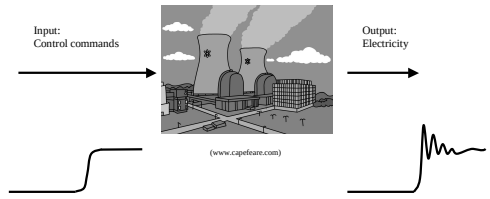
Helsinki University
of Technology

Introduction



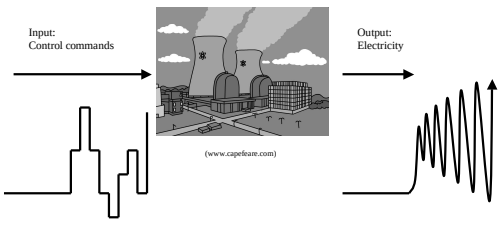
Helsinki University
of Technology

Introduction: Good guys



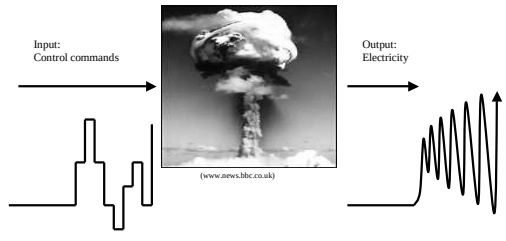
Helsinki University
of Technology

Introduction: Bad guys



Helsinki University
of Technology

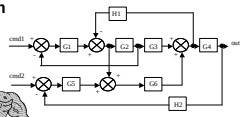
Introduction: Bad guys



Helsinki University of Technology

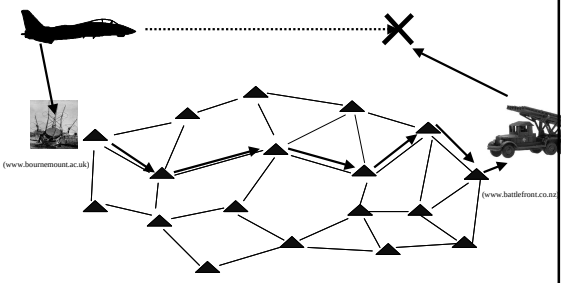
Background

- **Colonel John Boyd (1927-1999) OODA-loop**
  - **Model for human decision making**
- **Industrial control systems**
  - **Used in process control system**
  - **Based on benevolent nodes**
  - **Information comes with constant delay**
- **Brute force attacks**
  - **No brain, just muscles**
  - **Easy to detect**



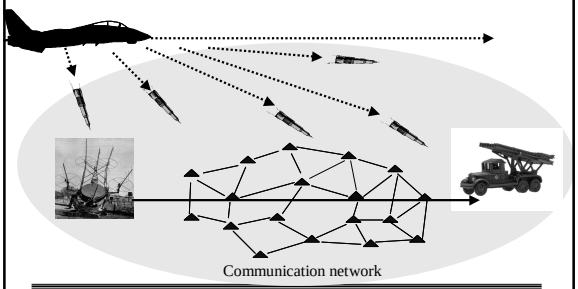
Helsinki University of Technology

Traditional approach: Defender wins



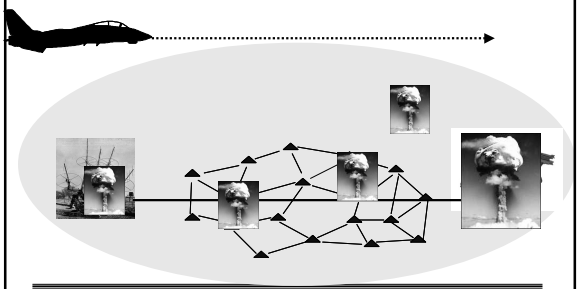
Helsinki University of Technology

Traditional approach example: Brute force



Helsinki University of Technology

Traditional approach example: Brute force



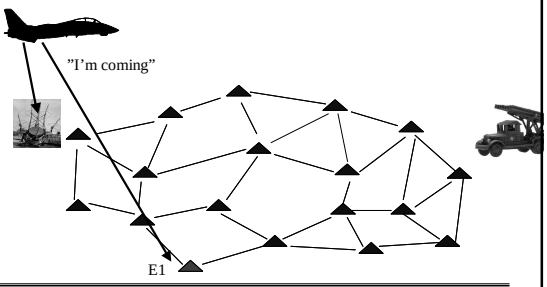
Helsinki University of Technology

Definition of a stealth attack (against computer network)

- **Network seems to operate under normal operating principles**
  - **At any time, behavior of all nodes (especially malevolent nodes) is according to expectations**
  - **Malevolent nodes do not generate any significant extra traffic**
- **Attack may be external or internal**
- **Results**
  - **Important messages are lost/delayed**
- **Enemy can reuse the same attack again and again**
- **Benevolent nodes may be blamed for misbehavior**

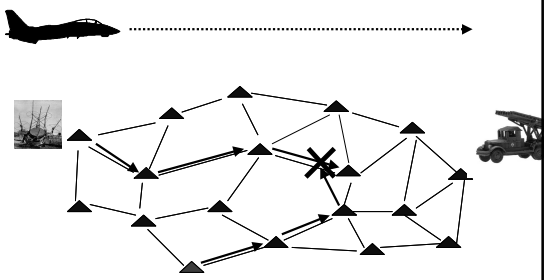
Helsinki University of Technology

Stealth attack: Attacker wins



Helsinki University of Technology

Stealth attack: Attacker wins



Helsinki University of Technology

Stealth attack methods

- **<u>It is the matter of information superiority</u>**
- **When we know, in advance, what will happen in the defender's network, we can easily block the traffic with minimum effort**
  - **Few seconds/fraction of seconds is enough to gain the advantage**
- **Attack can resemble to a ordinary network anomaly that may occur occasionally**
  - **Defender thinks that "it was Mr. Murphy again"**

Helsinki University of Technology

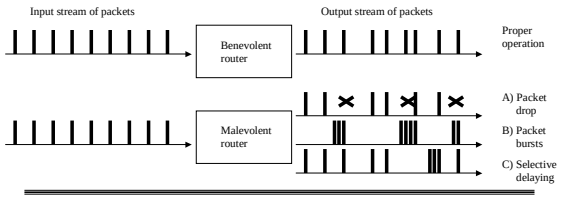
Stealth attack methods

- **Radio disturbance (easiest to detect)**
  - **Radio jamming/congestion**
- **Manipulated messages**
  - **Bit manipulation**
- **Dropped packets**
- **Network overload**
  - **Extra copies of the packet**
  - **Garbage generator**
- **Protocol disturbance**
  - **"I have a routing problem"**
  - **"I need to find a route to node X"**
- **Packet delaying (most difficult to detect)**

Helsinki University of Technology

Stealth attack methods

- **A proper packet delaying causes fluctuation on the network traffic**
  - **Simple example is TCP protocol's slow start effect**



Helsinki University of Technology

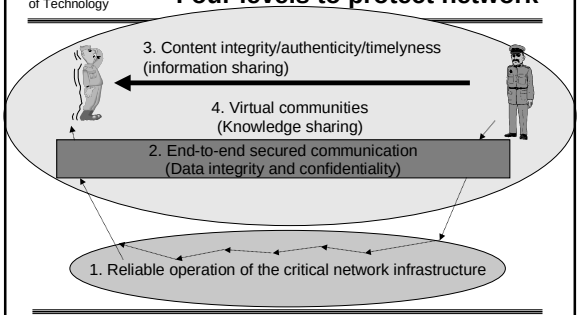
Protection methods

- **Security solutions to protect against**
  - **Wrong data**
  - **Altered data**
  - **Replayed data**
- **No protection against**
  - **Missing data**
  - **Delayed data**

⇒**Crucial role of the network infrastructure to carry legitimate packets promptly through the network in all conditions**

Helsinki University of Technology

Protection methods: Four levels to protect network



Helsinki University of Technology

Protection methods: Protecting infrastructure:

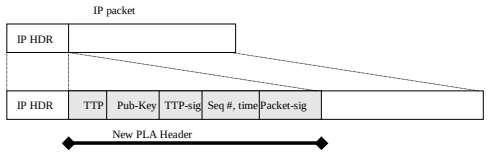
- **Target**
  - **Communication between two legitimate computers shall work in all the time**
    - **despite any hostile attacks, that manipulate packets, jam the network, cut the communication links, or by other means try to disturb legitimate communication**

  ⇒ The network (i.e., routers) shall distinguish whether a packet is
  - **generated by a legitimate computer (and packet shall be forwarded further)**
  - **generated or modified by attackers (record/discard that packet and optionally rise an alarm)**

  - **Network shall be capable of prioritizing traffic based on importance of packets (QoS) and user**
    - **not every computer or packet is equal**

Helsinki University of Technology

Protection methods: Packet level authentication (PLA)



PLA header inserted the same way as Mobile IP, IPsec, ... protocols

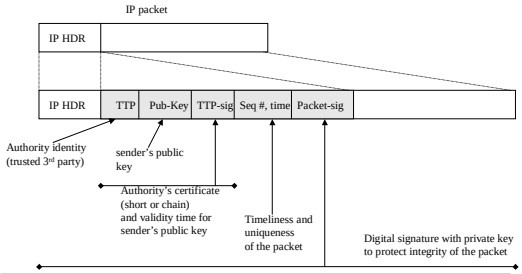
PLA header is transparent to standard IP routers (that do not understand PLA)

PLA header is transparent to all upper level protocols (UDP, TCP, SCTP, ...)

PLA can be used in both IPv4 and IPv6 networks

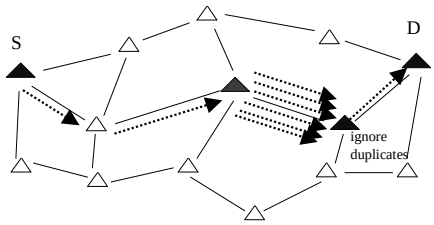
Helsinki University of Technology

Protection methods: Packet level authentication (PLA)



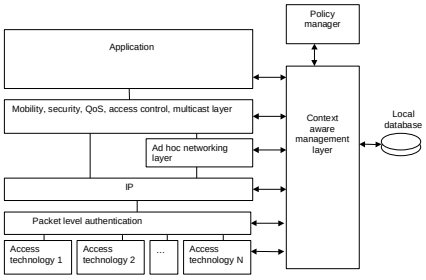
Helsinki University of Technology

Protection methods: PLA: Restricting replay attack



Helsinki University of Technology

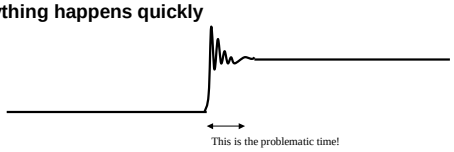
Protection methods: Context Aware Management/Policy Manager



Helsinki University of Technology

Protection methods: Dynamic trust management

- **Monitor all your neighbors' behavior**
- **Report anomalies**
- **Revoke malevolent nodes from the network**
- **...but this will not help in transient cases where everything happens quickly**



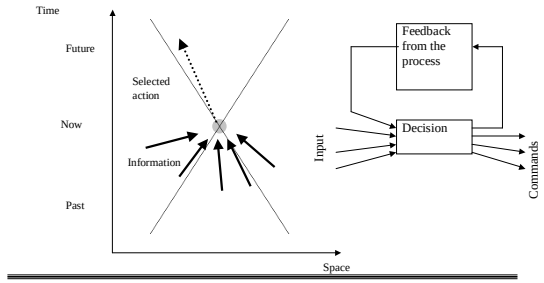
Helsinki University of Technology

Remaining problems

- **Statistical phenomena**
  - **How to predict, when a node is behaving maliciously?**
- **Unique cases**
  - **Can't collect statistically significant amount of information**
- **Amount of data**
  - **The glitch in the network may be caused by any packet**
- **No roll-back**
  - **Once the decision is made, it is often too late to go back**

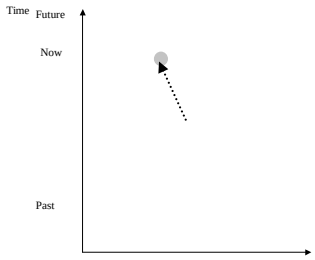
Helsinki University of Technology

A traditional memoryless decision process



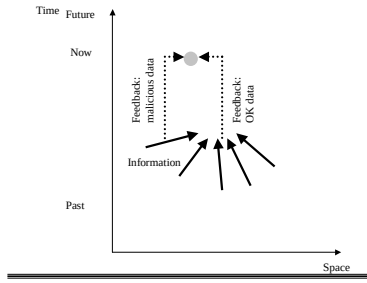
Helsinki University of Technology

A new decision process with memory and decision history



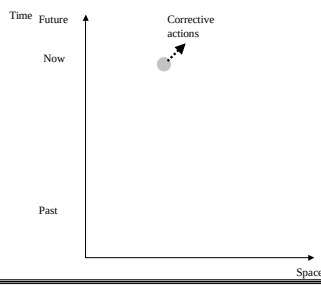
Helsinki University of Technology

A new decision process with memory and decision history



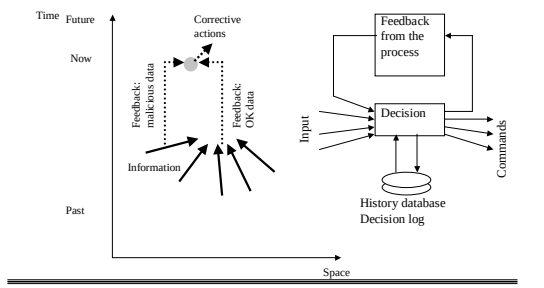
Helsinki University of Technology

A new decision process with memory and decision history



Helsinki University of Technology

A new decision process with memory and decision history



Helsinki University
of Technology

Conclusions

- **It is easy to disturb computer networks**
  - **With stealth attacks defender thinks that his network operates fine, and all anomalies are just random, statistical phenomena**
- **Some of the external attacks are quite easy to detect**
  - **Internal attacks (by compromised nodes) are the nasty ones**
- **A new decision making system is needed**
  - **that is capable of remaking decisions when previous decisions were made based on wrong or incomplete information**
  - **corrective actions are then needed!**

Helsinki University
of Technology

Thank you, Questions?