L.Reznik
Possible directions and topics

Thank you, Dr. Bischof, for inviting me

What is the future of CS?

1. **What will be the most important application area?**
2. **What will be the most widely used (and needed) methodology?**

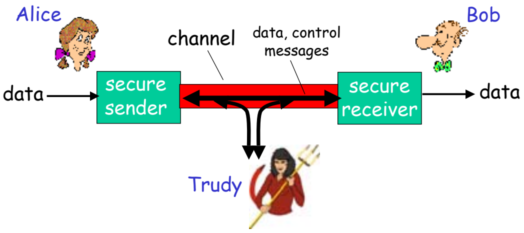
Security

Q: What is security?

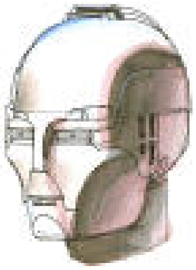
A: Security = C+I+A

Friends and enemies: Alice, Bob, Trudy

- well-known in network security world
- Bob, Alice (lovers!) want to communicate “securely”
- Trudy (intruder) may intercept, delete, add messages



Artificial Intelligence



Q: What is AI?

A: ???

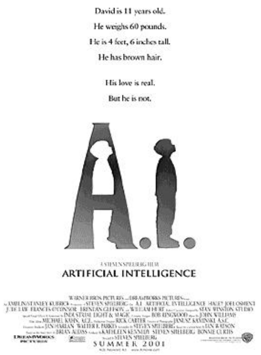
What is AI?

- Director:

Steven Spielberg

Stars: Jude Law, Haley Joel Osment, Frances O’Connor

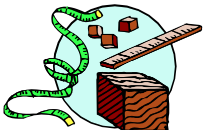
Plot: In the wake of an environmental disaster, a new kind of self-aware computer is created



What is AI again?:

- Although the term of AI has been widely used for quite a long time with steadily increasing amount of research and applications, there is no anonymously accepted definition. AI can mean many things to different people and various techniques are considered as belonging to AI.
- The term coined in 1956 by J. McCarthy at MIT
- Two branches: engineering discipline dealing with the creation of intelligent machines and empirical science concerned with the computational modelling of human intelligence
- The goal of AI is developing methods, which allow producing thinking machines that can solve problems
- Which problems?
- ill-defined and ill-structured
- complicated taxonomy or classifying
- Combinatorial optimisation

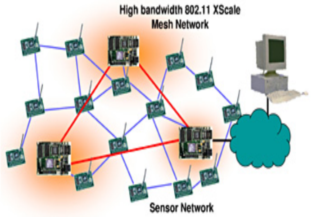
Association based security measurement and improvement in sensor networks



Direction 1

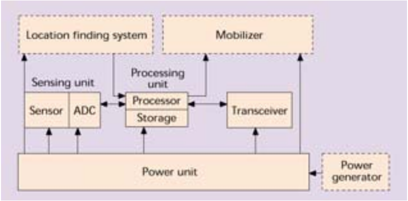
Sensor Networks

- Sensor networking is an emerging technology.
- In sensor networks, we have small sensor nodes which are densely deployed in an area.
- The sensor nodes equipped with transceiver such that they can send and receive information from neighboring nodes in the form of a wireless network



Sensor Nodes

- Sensors nodes are low power, low memory devices equipped with one or more sensors.
- A sensor node has four basic components



- Sensing unit
- Processing unit
- Transceiver unit
- Power unit

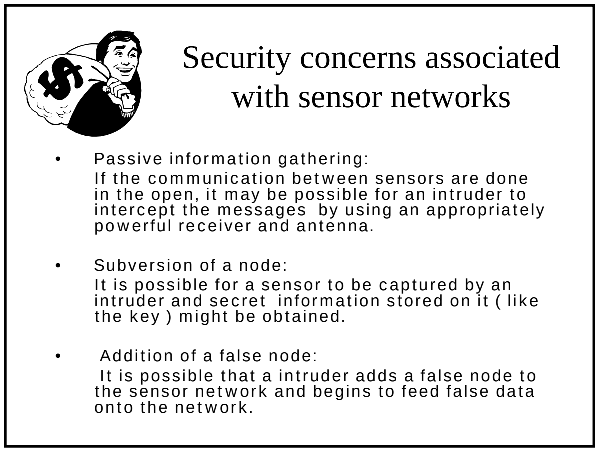
Sensor Networks and Ad-Hoc Networks

DIFFERENCES

- The sensor nodes in a sensor network are densely deployed and normally several times the number of nodes in a typical ad hoc network.
- Sensor nodes are prone to failure.
- The topology of a sensor network changes very frequently.
- Sensor nodes have limited power, computational capacities and memory.
- The sensor nodes may not have global identification (ID) because of the large amount of overhead and number of nodes

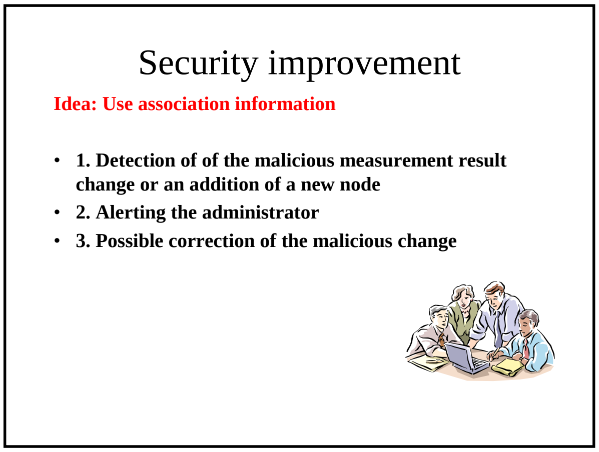
Security in Sensor Networks

- Since sensor networks are still an emerging technology, there is not much that has been done to address security in sensor networks
- Sensor networks are wireless networks.
- Wireless networks are typically more vulnerable to attack than wired network because of the way they transmit data.
- Also, wireless sensor networks have additional vulnerability because the nodes normally deployed in an environment which may be hostile or which is not physically protected.



Security concerns associated with sensor networks

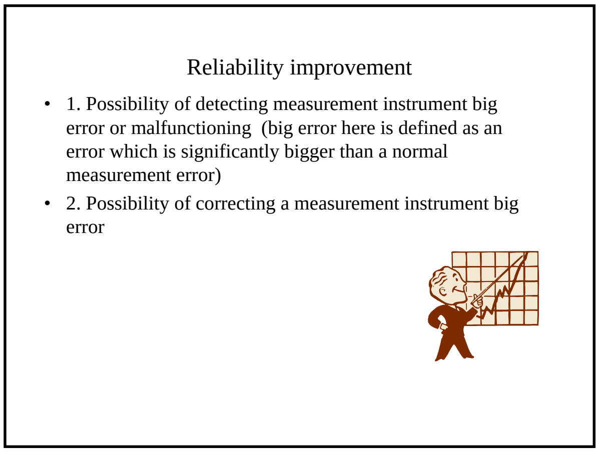
- Passive information gathering:
  If the communication between sensors are done in the open, it may be possible for an intruder to intercept the messages by using an appropriately powerful receiver and antenna.
- Subversion of a node:
  It is possible for a sensor to be captured by an intruder and secret information stored on it (like the key) might be obtained.
- Addition of a false node:
  It is possible that a intruder adds a false node to the sensor network and begins to feed false data onto the network.



Security improvement

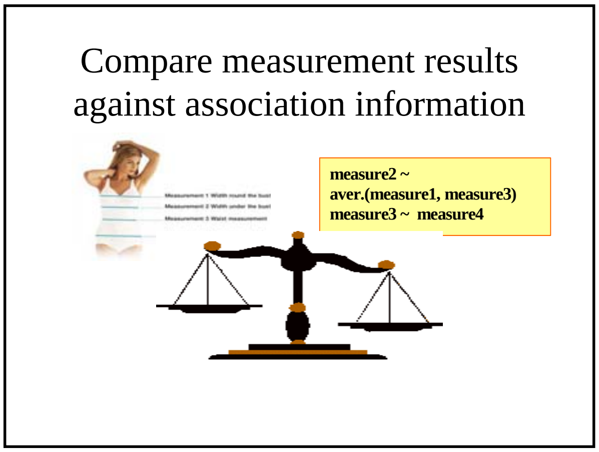
Idea: Use association information

- **1. Detection of of the malicious measurement result change or an addition of a new node**
- **2. Alerting the administrator**
- **3. Possible correction of the malicious change**



Reliability improvement

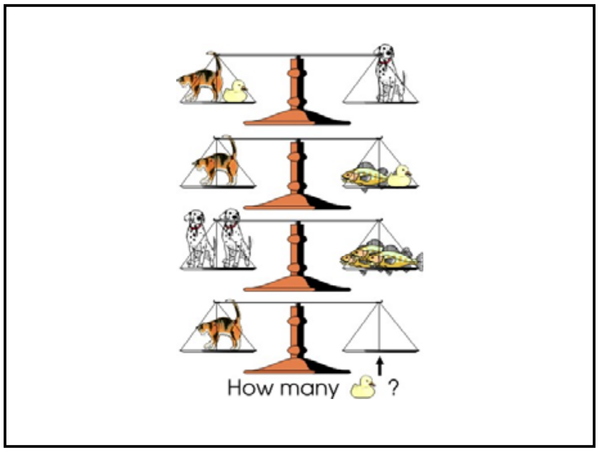
- 1. Possibility of detecting measurement instrument big error or malfunctioning (big error here is defined as an error which is significantly bigger than a normal measurement error)
- 2. Possibility of correcting a measurement instrument big error

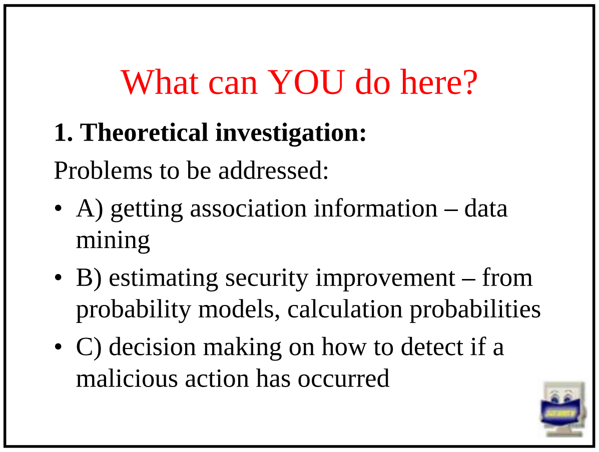


Compare measurement results against association information

Measurement 1 Width round the bust
Measurement 2 Width under the bust
Measurement 3 Waist measurement

**measure2 ~
aver.(measure1, measure3)
measure3 ~ measure4**





What can YOU do here?

1. Theoretical investigation:

Problems to be addressed:

- A) getting association information – data mining
- B) estimating security improvement – from probability models, calculation probabilities
- C) decision making on how to detect if a malicious action has occurred

What can YOU do here?

2. Simulation program:

Problems to be addressed:

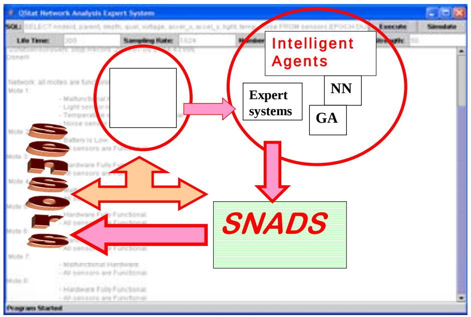
Design and implement the simulation environment to address problems formulated on the previous slide

Sensor Network Anomaly Detection System (SNADS)

- designed to become modular, extensible, robust, scalable and portable
- versatile cross platform tool
- modularity is mainly achieved via a central signaling system
- components are replaced and added on the fly : achieve scalability
- database subsystem provides a simple interface for data logging and searching
- intelligent agents generate new association informatin and modify existing one
- anomaly detection: detect and possibly correct measurements

Implementation

Protocol implementation: software



Implementation

Intelligent agents: NN in change detection

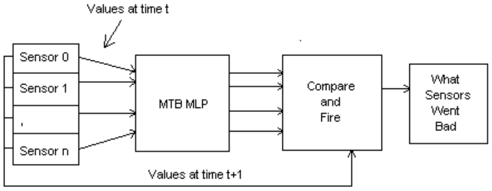


Fig. 4. This is the data flow for the novelty detection application..

Implementation

What can YOU do here?

3. GUI and Integrated Environment:

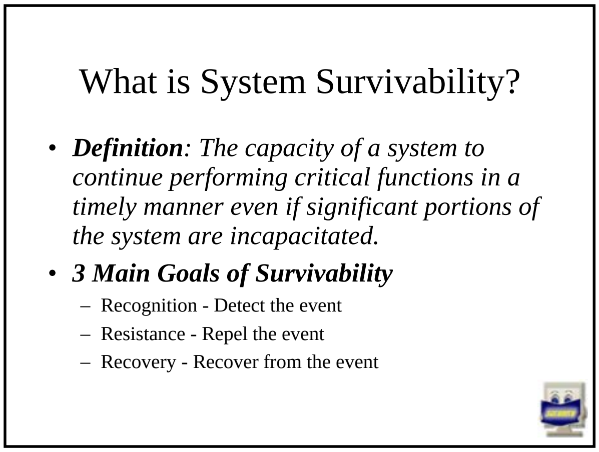
Problems to be addressed:

1.Design and implement a nice dynamic GUI for association information acquisition

2. Design and implement an Integrated Environment for information acquisition and simulation with dynamic change

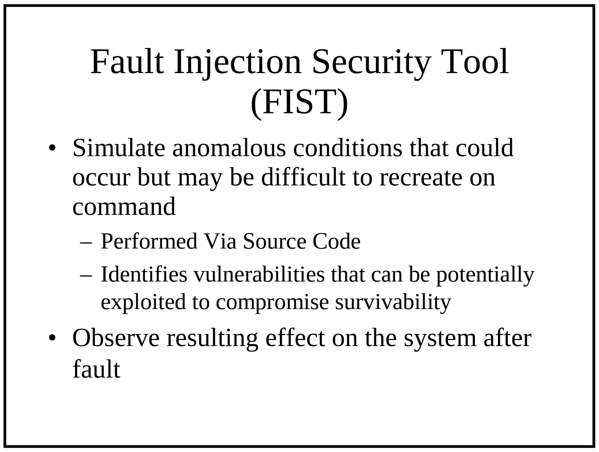
How to measure computer security?

- **Direction 2**
- **Topic A: Measuring system vulnerability and survivability through fault injection**



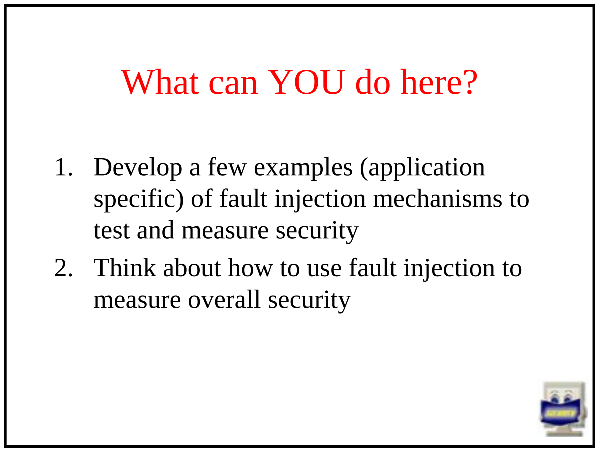
What is System Survivability?

- ***Definition****: The capacity of a system to continue performing critical functions in a timely manner even if significant portions of the system are incapacitated.*
- ***3 Main Goals of Survivability***
  - Recognition - Detect the event
  - Resistance - Repel the event
  - Recovery - Recover from the event



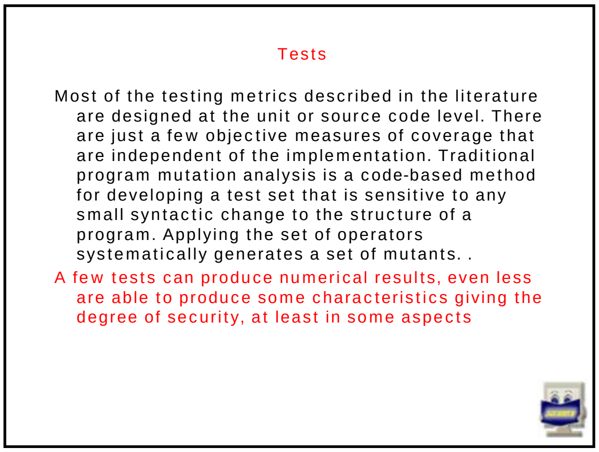
Fault Injection Security Tool (FIST)

- Simulate anomalous conditions that could occur but may be difficult to recreate on command
  - Performed Via Source Code
  - Identifies vulnerabilities that can be potentially exploited to compromise survivability
- Observe resulting effect on the system after fault



What can YOU do here?

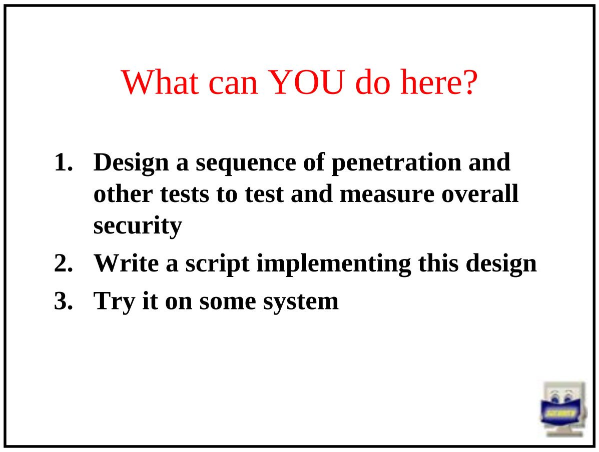
1. Develop a few examples (application specific) of fault injection mechanisms to test and measure security
2. Think about how to use fault injection to measure overall security



Tests

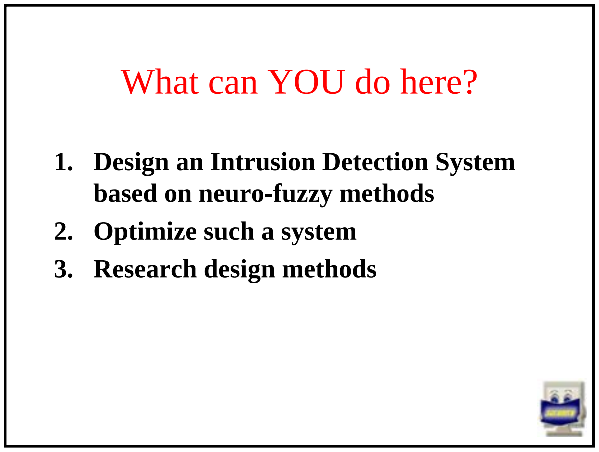
Most of the testing metrics described in the literature are designed at the unit or source code level. There are just a few objective measures of coverage that are independent of the implementation. Traditional program mutation analysis is a code-based method for developing a test set that is sensitive to any small syntactic change to the structure of a program. Applying the set of operators systematically generates a set of mutants. .

A few tests can produce numerical results, even less are able to produce some characteristics giving the degree of security, at least in some aspects



What can YOU do here?

1. **Design a sequence of penetration and other tests to test and measure overall security**
2. **Write a script implementing this design**
3. **Try it on some system**



What can YOU do here?

1. **Design an Intrusion Detection System based on neuro-fuzzy methods**
2. **Optimize such a system**
3. **Research design methods**

How to evaluate security tools?

- Direction 3

Tools analysis and classification

Authentication / Password	Network/Host Scanner	Intrusion Detection	Integrity-Checking	Service-Filtering	Encryption	Network Monitoring	FireWalls	Hardening OS
Smard Card	nmap	Snort Open Source	Trip Wire	TCP/IP Wrapper	PGP (GnuPG)	tcpdump	IP Filter	TIGER
OpenSSH	Nessus	Argus	MD5		IPsec	ethereal	FireWall-1	JASS (Solaris)
ppp(CHAP)	ISS	swatch	Fingerprint Database (for Solaris)		SSL	snoop	PIX	YASSP (for Solaris)
Kerberos V5	SAINT	arpwatch	SHA1		STUNNEL		SunScreen	STEP by STEP (e.g. SANS's)
Biometric	SARA	Gabriel					Outpost	
sudo		Log File						
RBAC		Hog-watch						
		PortSentry						
		Shadow						

Tools analysis and classification

As the security tools are broadly classified into five parts

Therefore before selecting any tool various points should

be kept which are follows :

- System requirement
- Network topology
- Financial constraints
- Type of application
- Target organization (defense , hospital ...)

And many more

➢ Therefore the user has to do the tradeoffs between the tools while selecting it.

What can YOU do here?:

1. Comparison and evaluation of a few specialized tools
2. Development of the methodology how to compare tools
3. Writing a script implementing 2

More practical work: providing physical security with sensor networks

- Direction 4

What can YOU do here?

1. **Install hardware and software from Crossbow Inc.**
2. **Make it work**
3. **Develop application software**