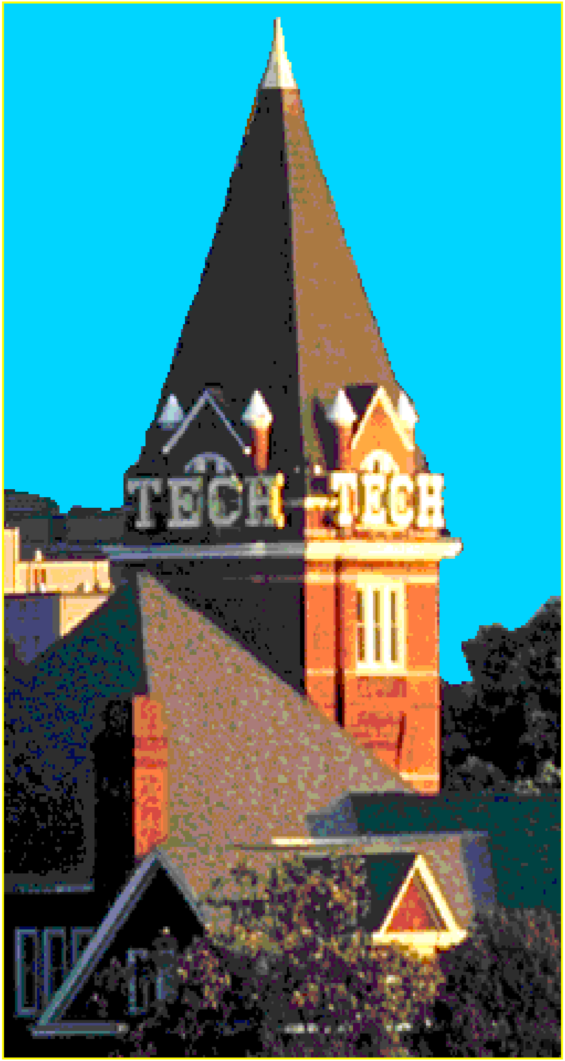


NEW METHODS OF INTRUSION DETECTION USING CONTROL-LOOP MEASUREMENT

May 16, 1996

Myron L. Cramer, James Cannady, and Jay Harrell
myron.cramer@gtri.gatech.edu
Georgia Tech Research Institute
Georgia Institute of Technology
Atlanta, Georgia 30332

PURPOSE

- The purpose of this presentation is to describe some new ideas in intrusion detection.
- These ideas are based upon a review of the physics of the problem and an analysis of applicable technological approaches.
- The proposed new methods reflect concepts still in development and evaluation by the authors.

TOPICS

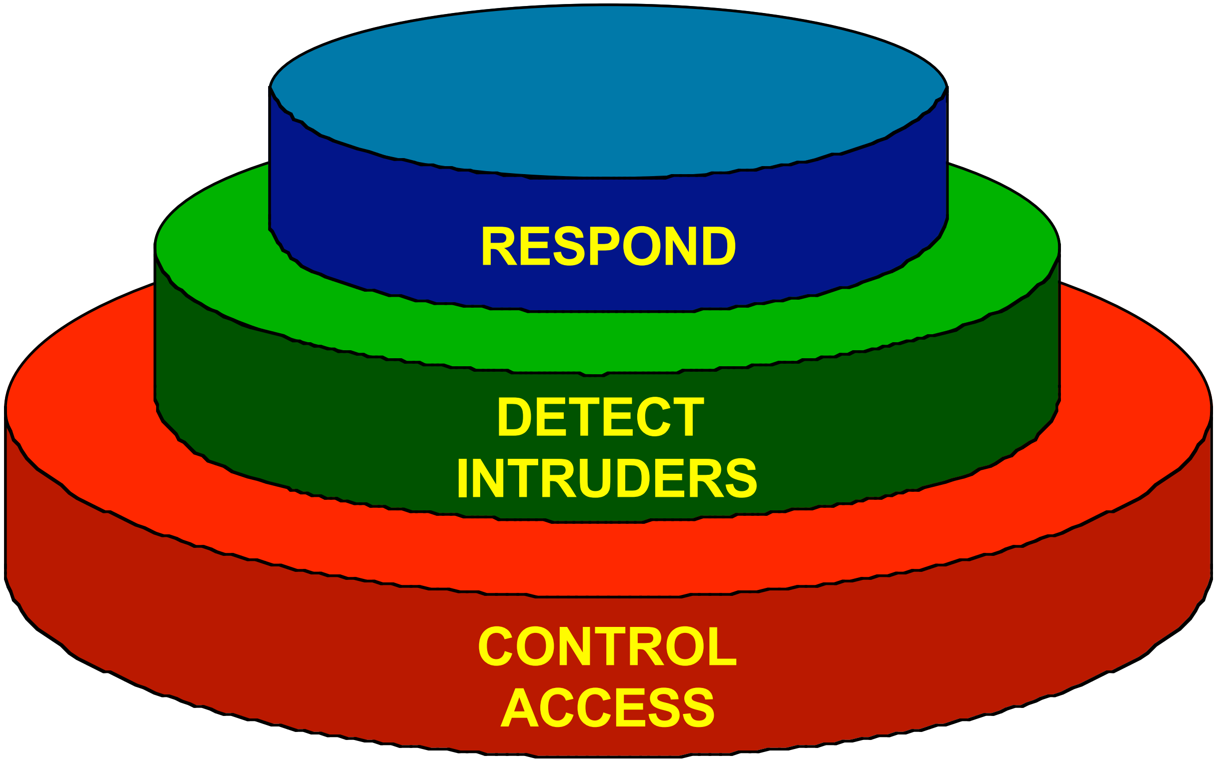
This presentation includes a discussion of the:

- Need for better Intrusion Detection Systems (IDS)
- Intrusion Detection Operational Concepts
- Applicability of Digital Signal Processing to Intrusion Detection
- Control-Loop Concepts
- Use of the above in an Intrusion Detection System
- Benefits of Approach

Georgia Tech Research Institute

ROLE OF INTRUSION DETECTION

Intrusion detection systems are the second layer of protection.



IDEAL INTRUSION DETECTION SYSTEM

The ideal intrusion detection system has the following characteristics:

- timeliness
- high probability of detection
- low false-alarm rate
- specificity in attack characterization
- scalability to large (infinite) networks
- requires a minimum of a priori information about potential attackers and their methods

Georgia Tech Research Institute

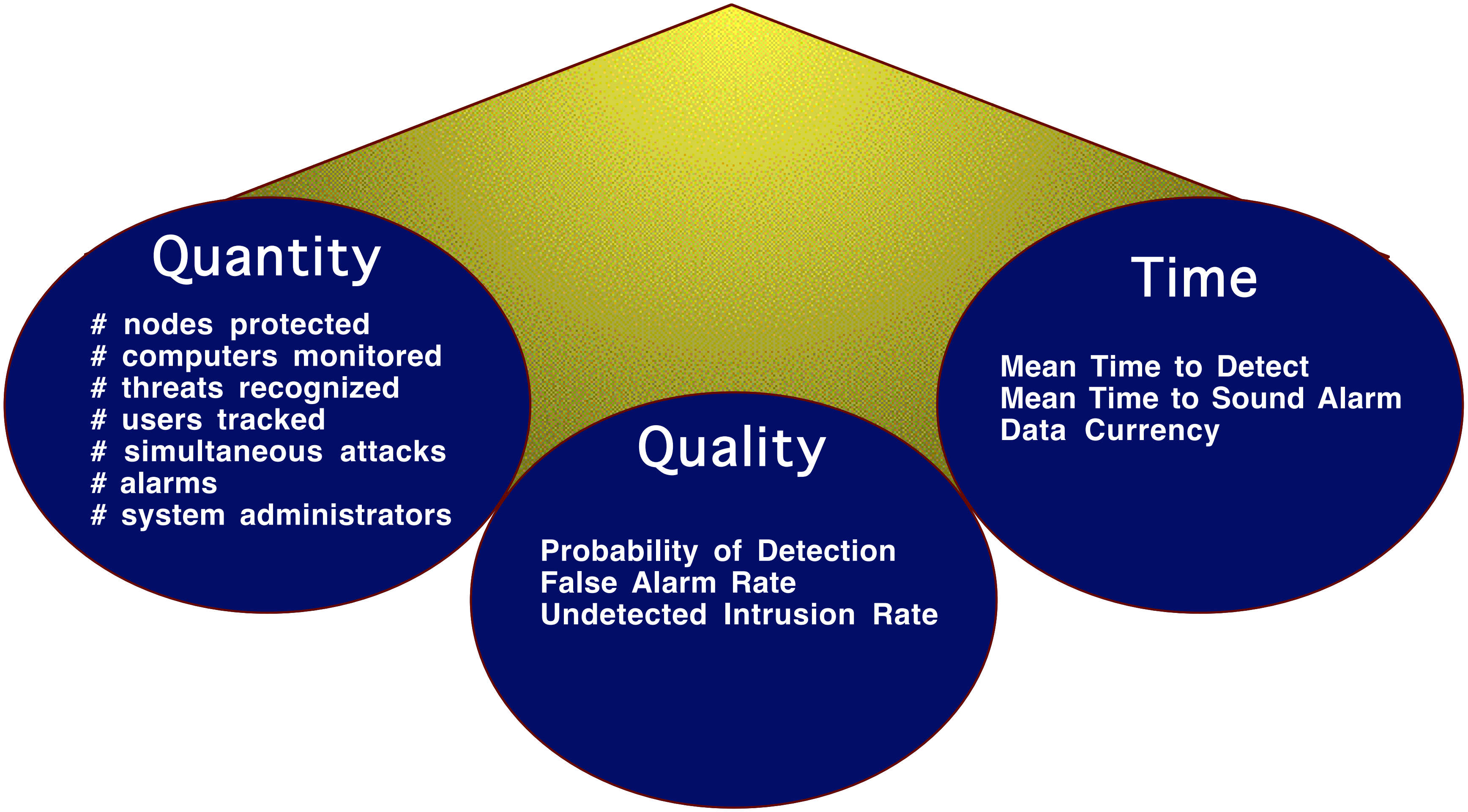
NEED FOR BETTER INTRUSION DETECTION SYSTEMS

- Inherent Penetrability of networked computers
  - » No access control system can preclude intrusions
- Available IDS are limited
  - » Better ⇒ higher detection probability, lower false alarm rate, more timely warning (real-time), lower processing burden, lower management burden, reduced demand for a priori data, more secure, less cumbersome, wider applicability, better coverage zones, …

Georgia Tech Research Institute

METRICS

There are three fundamental metrics:



Quantity

- # nodes protected
- # computers monitored
- # threats recognized
- # users tracked
- # simultaneous attacks
- # alarms
- # system administrators

Quality

Probability of Detection
False Alarm Rate
Undetected Intrusion Rate

Time

Mean Time to Detect
Mean Time to Sound Alarm
Data Currency

SCOPE

Scope is important.

- System to be Protected
- Attackers
- Intrusion Activity

Georgia Tech Research Institute

SYSTEM TO BE PROTECTED

The protected system can be an individual machine or a network of machines

- The problem arises in trying to protect a network by having to protect each machine in the network.
- Protecting the network can be more important than protecting some of the processors!

Georgia Tech Research Institute

ATTACKERS

There are wide differences in the types of possible threats.

- Degree of Attacks
  - Hacker
  - “Type II Information Warfare Attack”
- An attack may compromise:
  - confidentiality
  - authentication
  - integrity
  - availability of services

Georgia Tech Research Institute

“STANDARD” CLASSIFICATIONS

Intrusion detection systems are classified into the following categories:

- Statistical Anomaly Detection
- Rule-based Anomaly Detection
- Rule-based Penetration Identification

The new methods discussed in this paper do not fit in any of these categories!

Georgia Tech Research Institute

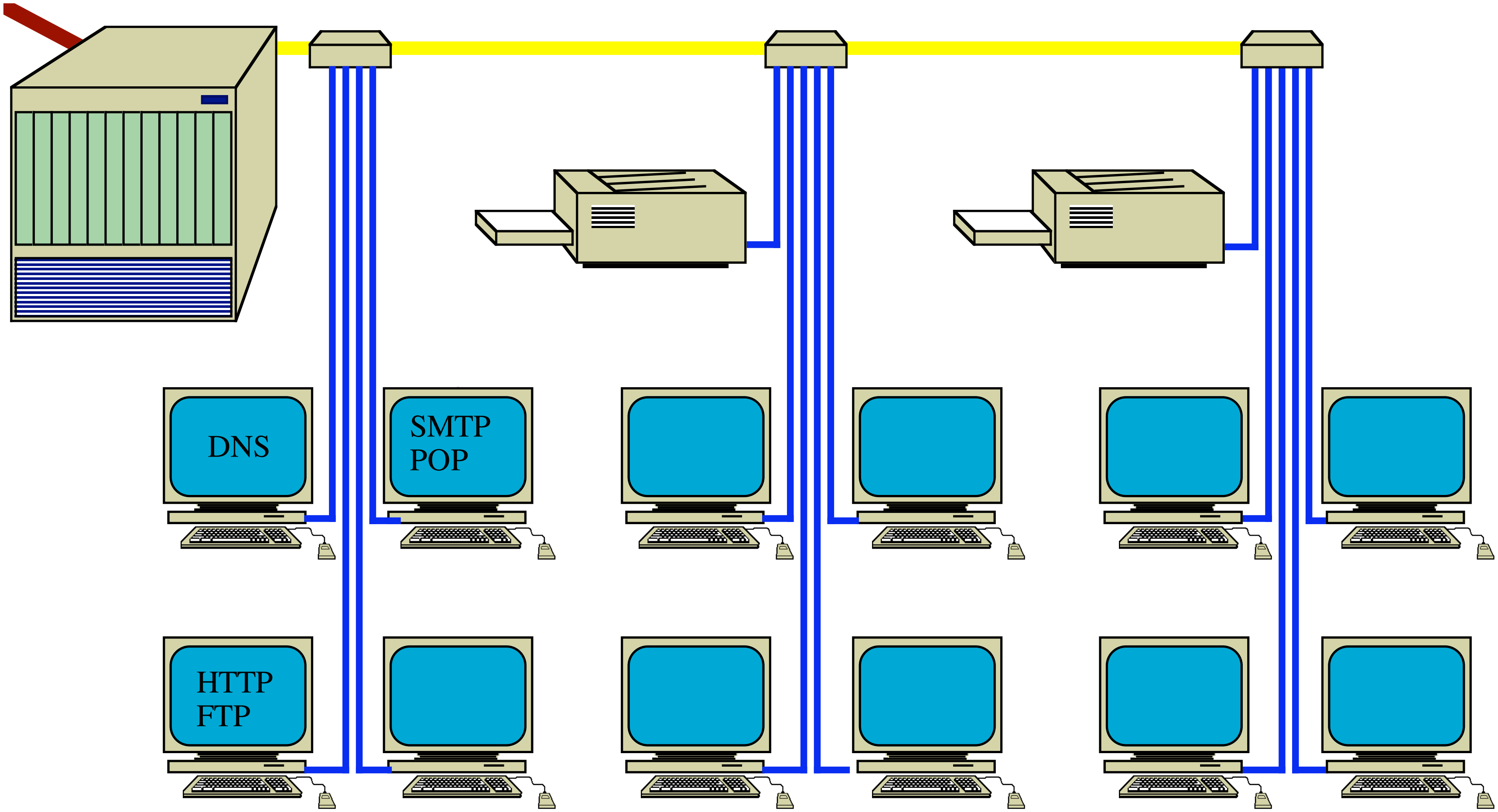
TYPES OF INTRUSION DETECTION SYSTEMS

Intrusion detection systems can be characterized by:

- Where they live
- What you have to tell them
- What they look for
- Which technologies they use
- What they tell you

WHERE THEY LIVE...

There are several choices of hosts for an IDS:


DNS
SMTP
POP
HTTP
FTP

WHERE THEY LIVE...

Intrusion detection systems can reside:

(1) on the computer(s) being protected

- » scaling problems for large networks: installation, configuration, and management of distributed IDSs
- » has poor visibility of related network activity
- » has best visibility for the IDS host computer

(2) on a separate processor strategically attached to the network

Georgia Tech Research Institute

- » advantages for large networks: installation, configuration, management
- » has best visibility of the overall network

WHAT YOU HAVE TO TELL THEM ...

The fundamental problem is the detection criteria for an "intrusion".

- Scenarios of attack, penetration
- User profiles
- Expected system usage

WHAT THEY LOOK FOR ...

In looking for intrusions, the IDS examines:

- Computer log files (historical)
- Process activities (real-time)

... then looks for matches with:

- Scenarios of attack, penetration

... or anomalies with:

- User profiles

A good criteria needs to be predictive!

INTRUSION ACTIVITY

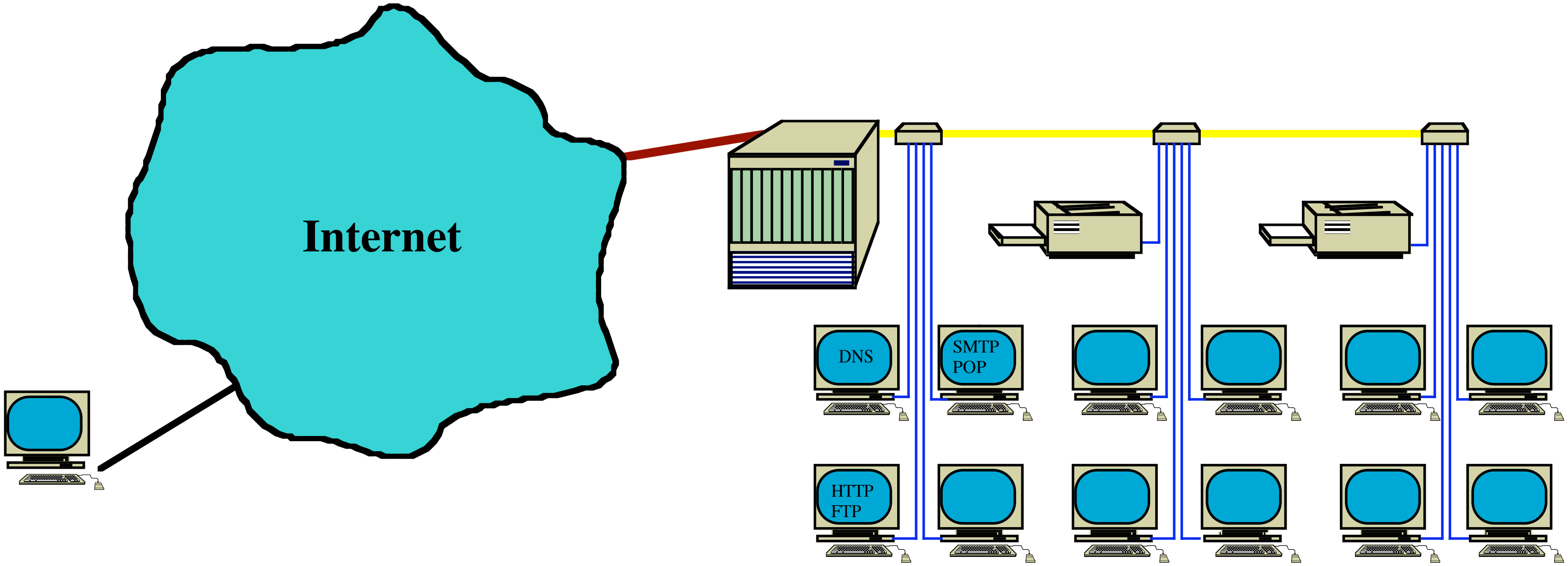
The problem:

- A determined attacker effects his intrusion through a sequence of activities to achieve a desired result.
- Each of these actions, viewed by itself may be a normal legitimate activity.
- It is only when this sequence is assembled that the intruder's hostile objectives become clear.

The core of the intrusion detection problem is how to recognize this behavior.

WHAT IS AN INTRUSION?

Intrusions can come in many ways.



- Sources
- Objectives
- Targets
- Actions

Georgia Tech Research Institute

- Knowledge
- Methods

WHICH TECHNOLOGIES THEY USE ...

Technologies for intrusion detection systems include:

- Data Base Methods
- Expert systems:
  - Rule-based
  - Case-based
  - Neural networks
- Digital Signal processing
  - Digital filters
  - Spectrum analysis

A good method needs to be adaptable!

Georgia Tech Research Institute

DIGITAL SIGNAL PROCESSING (DSP)

Digital signal processing is a technology-driven field.

- Processing of *discrete-time signals* or time series data sequences
- includes digital filters and spectrum analysis

Premise: DSP is applicable to IDS.

Georgia Tech Research Institute

APPLICATIONS OF DSP

- Widely used in many applications of electrical and computer engineering, including:
  - » modern control systems
  - » sensors and communications
- Using modern statistical methods, time-series data are:
  - » collected, filtered, correlated, and analyzed for many purposes including event detection
- The recognition and characterization of computer network protocols has been among the applications successfully handled by DSP

TIME SERIES DATA

Network Traffic includes Time Series Data.

```
01111110  11000000              XXXXXXXX            (INFO)             XXXXXXXXXXXXXXX       01111110      SLP
01111110  10000000              XXXXXXXX            (INFO)             XXXXXXXXXXXXXXX       01111110      SLP
01111110  11110000              XXXXXXXX            (INFO)             XXXXXXXXXXXXXXX       01111110      MLP
01111110  11100000              XXXXXXXX            (INFO)             XXXXXXXXXXXXXXX       01111110      MLP
```

» time series data contains patterns that implement the structures of the protocols

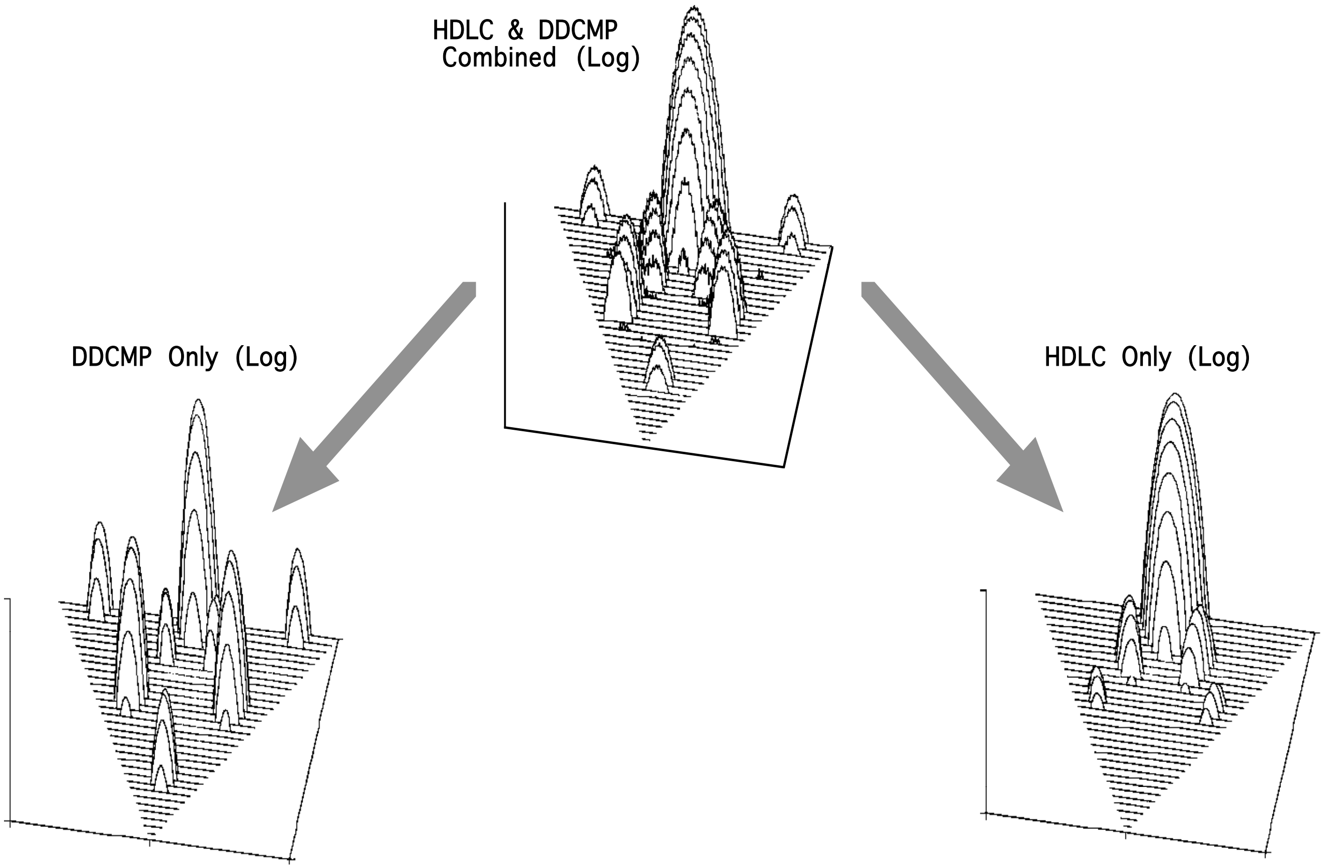
» DSP methods include integrating time-series data streams using digital models designed to correlate or weight activities of interest and to filter out uninteresting data

» interesting factors may be combinations of external addresses and certain combinations of processes

Georgia Tech Research Institute

PROTOCOL ANALYSIS

Statistical signal processing can be used to decompose protocol structures.



HDLC & DDCMP Combined (Log)

DDCMP Only (Log)

HDLC Only (Log)

Credit: Booz, Allen & Hamilton Inc.

CONTROL LOOP MEASUREMENT

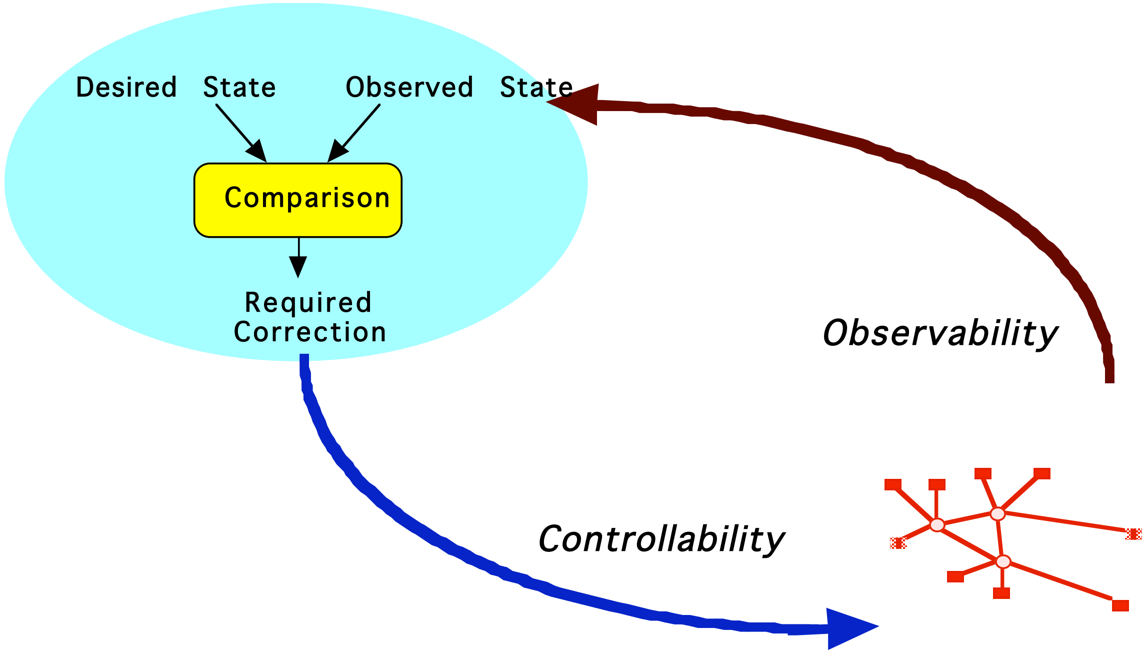
Hypothesis:

There is a new intrusion detection criteria utilizing the signature of an intruder's control-loop.

- A control-loop is characterized by both **observability** (surveillance) in conjunction with **controllability** (process accesses and system calls).
- We illustrate how to quantify this control and how to apply the resulting measure to discriminate intruders from normal activities.

CONTROL-LOOP DETECTION

Control:

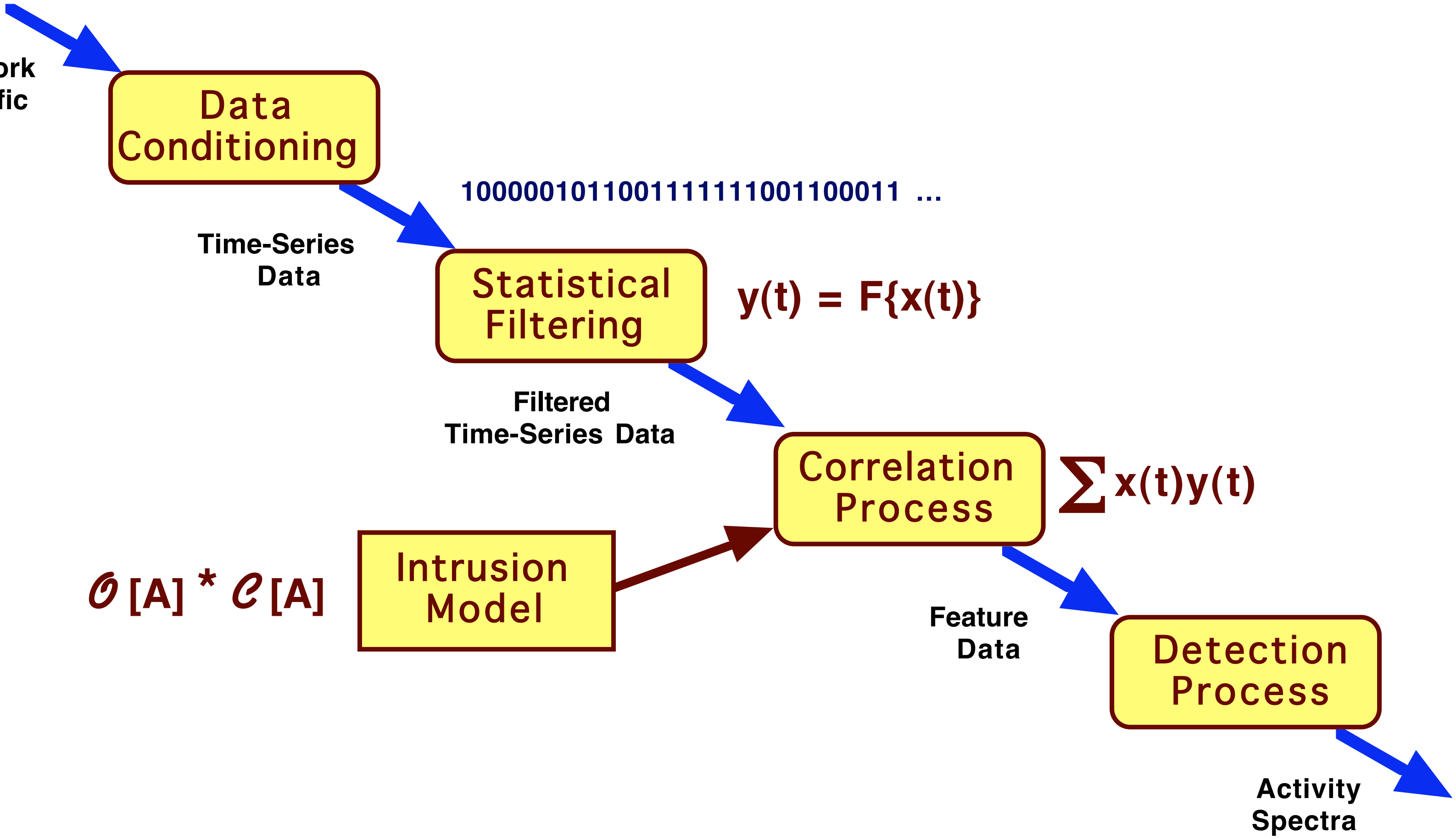


- characterized by observability (surveillance) in conjunction with controllability (process access and system calls)
- premise is that “high control behavior” provides a useful metric for discriminating interesting activities
- High levels of *control* may be used to recognize intruders

» High control behavior can be statistically detected in the bi-directional data flows using DSP

FUNCTIONAL CONCEPT

The functional concept includes a sequence of processes of network traffic to generates real-time activity spectra.



Network Traffic

Data Conditioning

Time-Series Data

1000001011001111111001100011 ...

Statistical Filtering

$y(t) = F\{x(t)\}$

Filtered Time-Series Data

Correlation Process

$\sum x(t)y(t)$

$\mathcal{O}[A] * \mathcal{C}[A]$

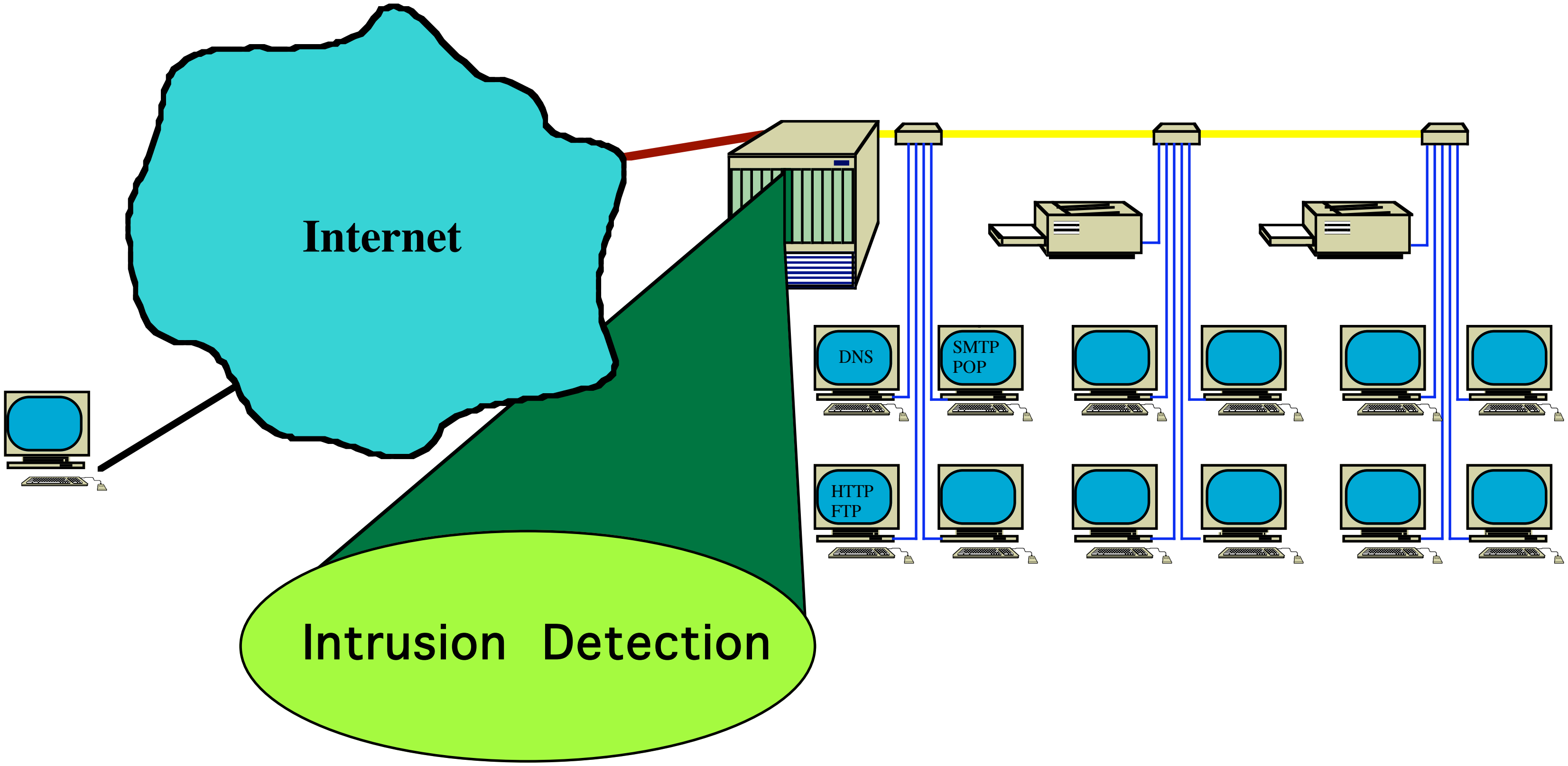
Intrusion Model

Feature Data

Detection Process

Activity Spectra

OPERATIONAL CONCEPT



Georgia Tech Research Institute

WHAT THEY TELL YOU ...

Spectral analysis:

- distribution of external connections
- internal distribution of correlated connections
- scale indicators of suspicious activity
- high degrees of observability and controllability

BENEFITS

Potential benefits of these new methods include:

- higher detection probability
- lower false alarm rate
- more timely warning (real-time)
- lower processing burden
- lower management burden
- reduced demand for a priori data
- more secure
- less cumbersome
- wider applicability

- better coverage zones

SUMMARY

We have discussed the:

- Need for better Intrusion Detection Systems (IDS)
- Intrusion Detection Operational Concepts
- Applicability of Digital Signal Processing to Intrusion Detection
- Control-Loop Concepts
- Use of the above in an Intrusion Detection System
- Benefits of Approach