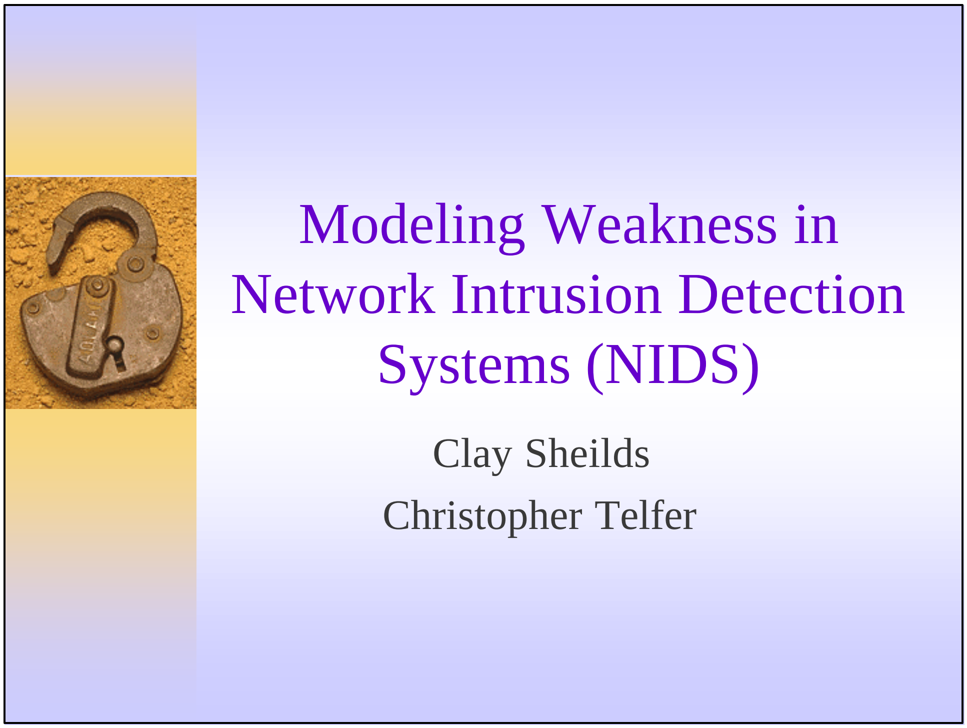
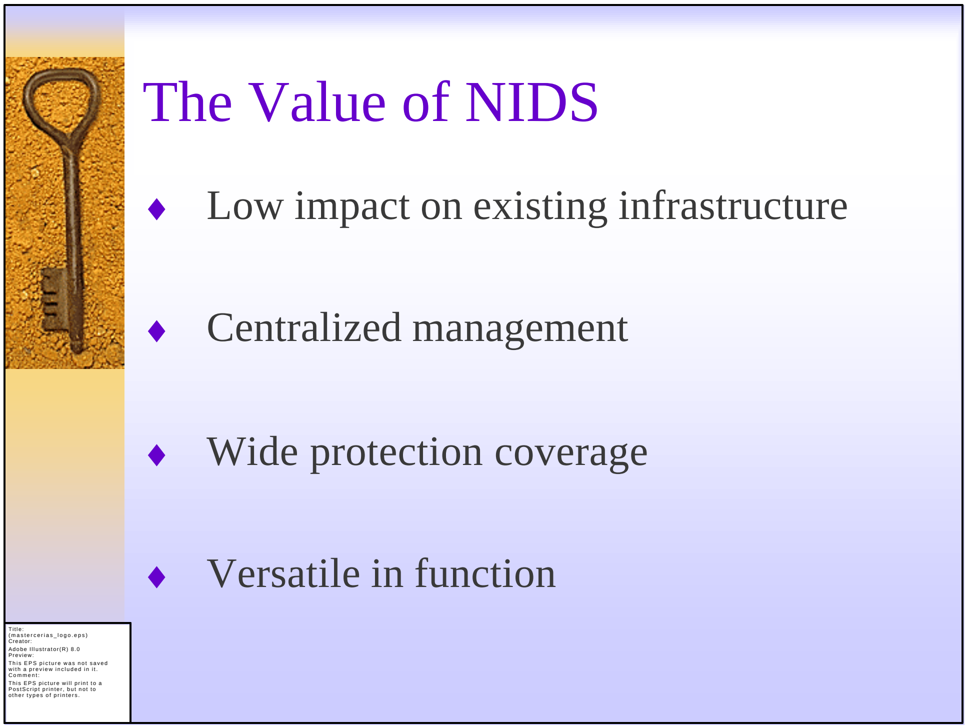


Modeling Weakness in Network Intrusion Detection Systems (NIDS)

Clay Sheilds

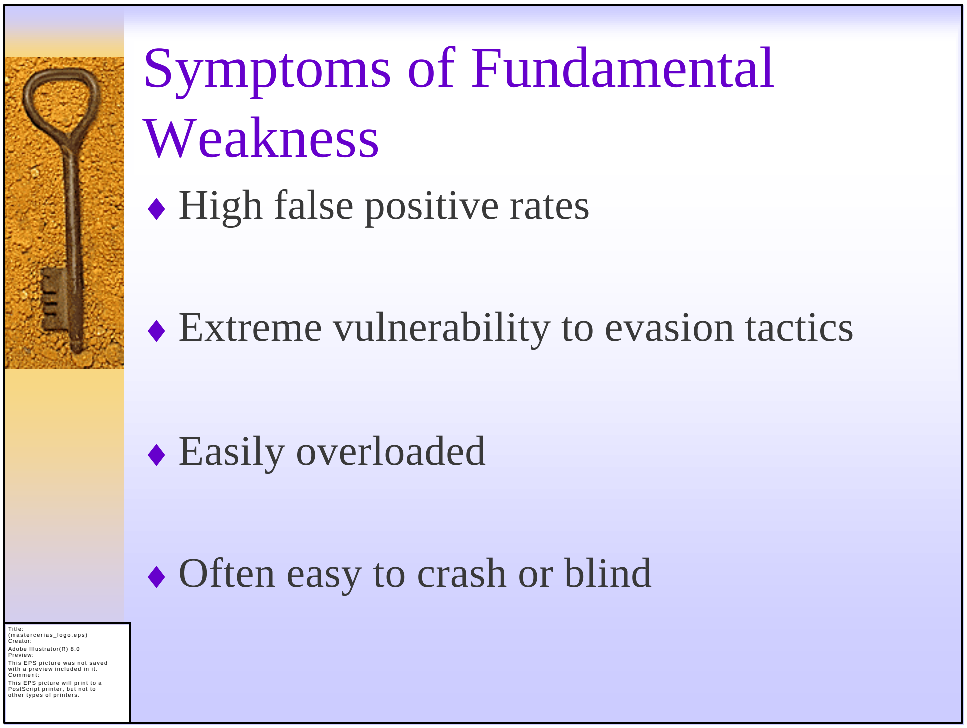
Christopher Telfer



The Value of NIDS

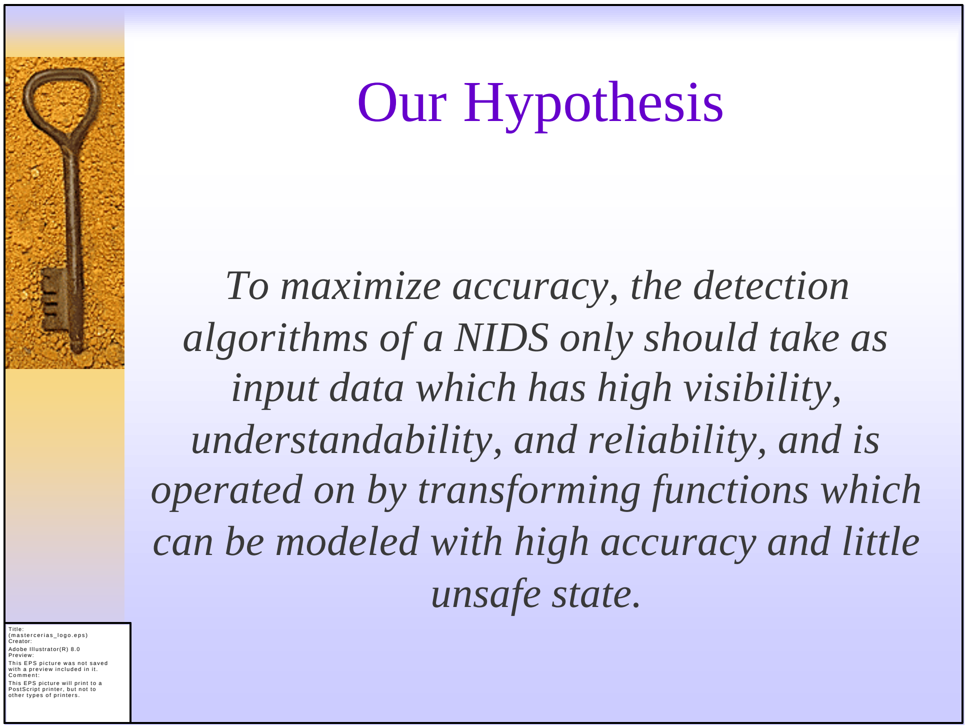
- Low impact on existing infrastructure
- Centralized management
- Wide protection coverage
- Versatile in function

Title:
(mastercerias_logo.eps)
Creator:
Adobe Illustrator(R) 8.0
Preview:
This EPS picture was not saved
with a preview included in it.
Comment:
This EPS picture will print to a
PostScript printer, but not to
other types of printers.



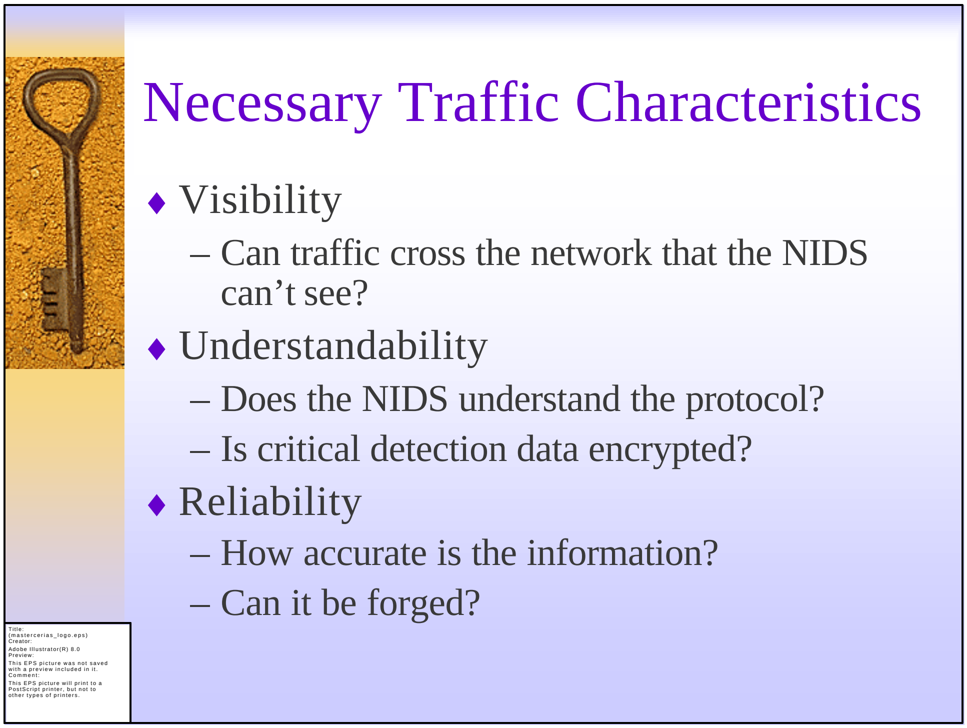
Symptoms of Fundamental Weakness

- High false positive rates
- Extreme vulnerability to evasion tactics
- Easily overloaded
- Often easy to crash or blind



Our Hypothesis

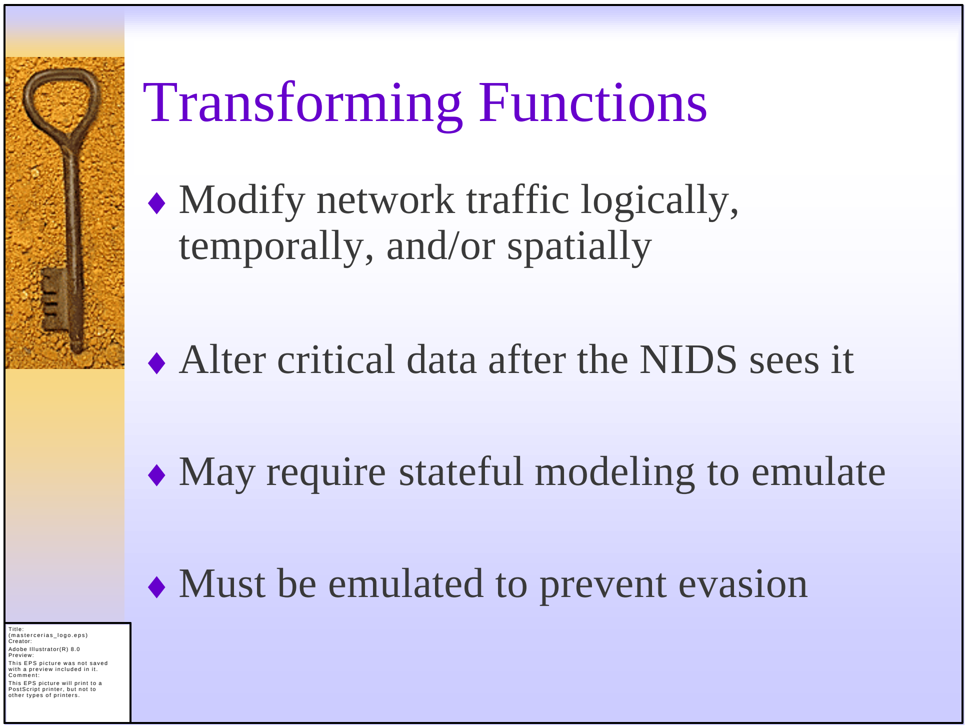
To maximize accuracy, the detection algorithms of a NIDS only should take as input data which has high visibility, understandability, and reliability, and is operated on by transforming functions which can be modeled with high accuracy and little unsafe state.



Necessary Traffic Characteristics

- Visibility
  - – Can traffic cross the network that the NIDS can’t see?
- Understandability
  - – Does the NIDS understand the protocol?
  - – Is critical detection data encrypted?
- Reliability
  - – How accurate is the information?
  - – Can it be forged?

Title:
(mastercerias_logo.eps)
Creator:
Adobe Illustrator(R) 8.0
Preview:
This EPS picture was not saved
with a preview included in it.
Comment:
This EPS picture will print to a
PostScript printer, but not to
other types of printers.



Transforming Functions

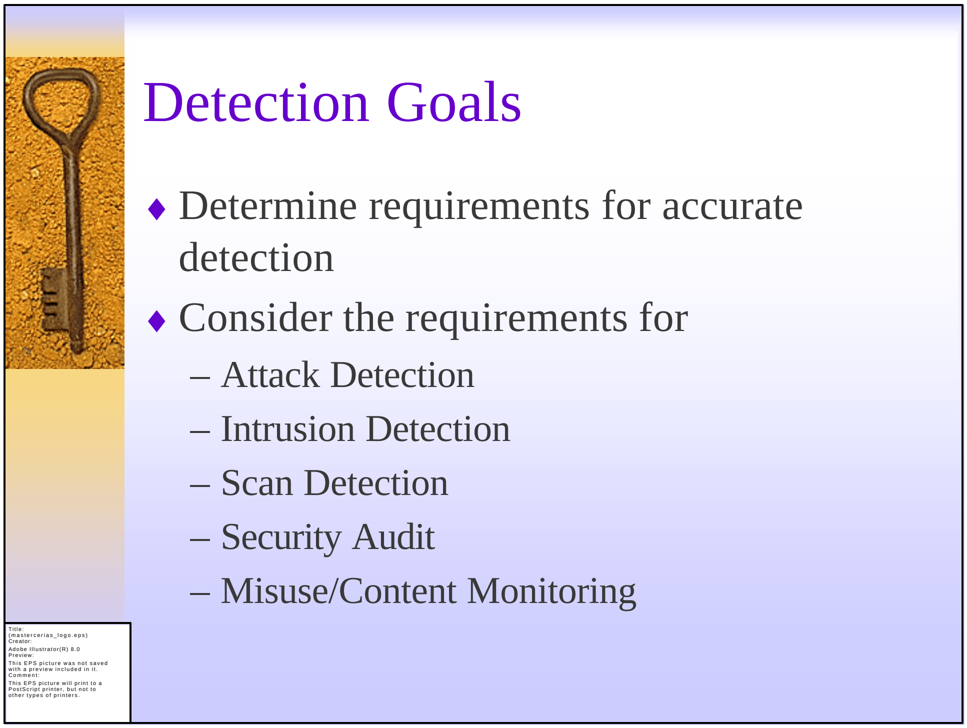
- Modify network traffic logically, temporally, and/or spatially
- Alter critical data after the NIDS sees it
- May require stateful modeling to emulate
- Must be emulated to prevent evasion

Title:
(mastercerias_logo.eps)
Creator:
Adobe Illustrator(R) 8.0
Preview:
This EPS picture was not saved
with a preview included in it.
Comment:
This EPS picture will print to a
PostScript printer, but not to
other types of printers.

Research Goals

- Apply our model to existing systems to discover weak points in their design
- Show how to modify algorithms or operating environments to improve accuracy
- Evaluate the feasibility of detection goals
- Provide system requirements given detection goals
- Eventually be able to estimate accuracy in NIDS

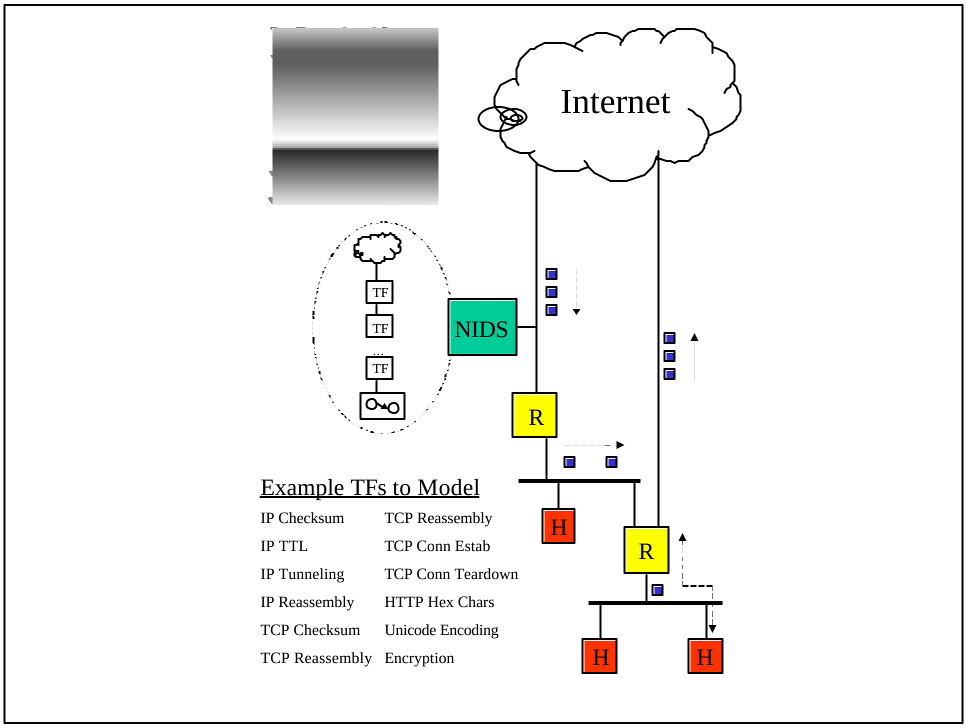
Title:
(mastercerias_logo.eps)
Creator:
Adobe Illustrator(R) 8.0
Preview:
This EPS picture was not saved
with a preview included in it.
Comment:
This EPS picture will print to a
PostScript printer, but not to
other types of printers.



Detection Goals

- Determine requirements for accurate detection
- Consider the requirements for
  - Attack Detection
  - Intrusion Detection
  - Scan Detection
  - Security Audit
  - Misuse/Content Monitoring

Title:
(mastercerias_logo.eps)
Creator:
Adobe Illustrator(R) 8.0
Preview:
This EPS picture was not saved
with a preview included in it.
Comment:
This EPS picture will print to a
PostScript printer, but not to
other types of printers.



Example TFs to Model

IP Checksum
IP TTL
IP Tunneling
IP Reassembly
TCP Checksum
TCP Reassembly

TCP Reassembly
TCP Conn Estab
TCP Conn Teardown
HTTP Hex Chars
Unicode Encoding
Encryption