

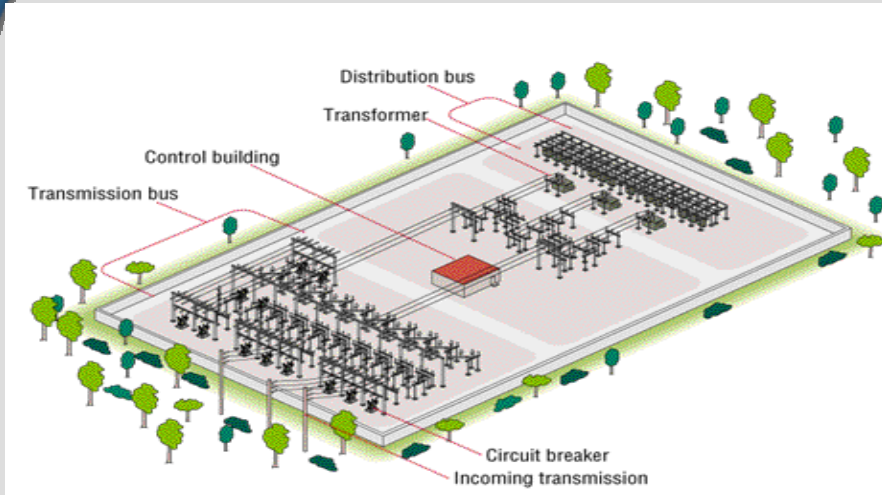
The Role of Authenticated Communications for Electric Power Distribution

Mark Hadley

Beyond SCADA
November 8 & 9, 2006
Pittsburgh, PA

The Research Challenge

Nonintrusive, lightweight message authentication for control systems



CONTROL

- Generator Set Points
- Manual Breaker controls

DATA

- Breaker Status
- Realtime Analogs Status



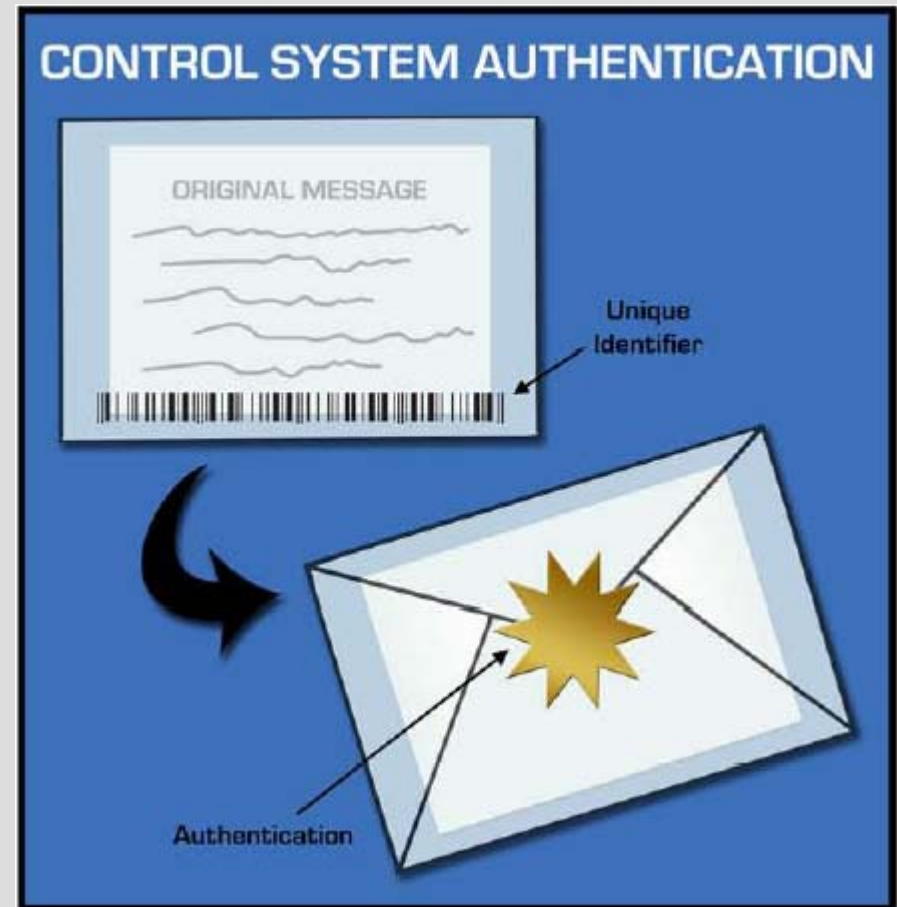
NERC Quote

▶ NERC Control Systems Security Working Group (CSSWG)

Control Systems are the “brains” of the control and monitoring of the bulk electric system and other critical infrastructures, but they were designed for functionality and performance, not security. Most Control Systems assume an environment of complete and implicit trust.

The Solution

- ▶ Provide trust through authentication
- ▶ Do not modify the original message
- ▶ Must not use encryption



Status

- ▶ Algorithm development
 - Two key update methodologies completed
 - Session negotiation
 - Hashing provided by Sha-1 or Sha-256
- ▶ Architecture
 - Embedded software
 - Industrial PC
 - Microcontroller
 - Event collection and reporting

Status – Con't

- ▶ Embedded software for I/O server is complete
- ▶ Industrial PC “bump in the wire” is complete
- ▶ Microcontroller solution is complete
- ▶ Syslog interface is complete
- ▶ Field test completed
 - Hosted by CenterPoint Energy
 - Protected communication to 3 production substations

The Role of Authenticated Communications for Electric Power Distribution

Mark Hadley

Mark.Hadley@pnl.gov

Beyond SCADA

November 8 & 9, 2006

Pittsburgh, PA