Security Issues for the Power Automation Industry in Central/South America

Juan Esteban Hoyos Pareja
Timothy X. Brown
Mark Dehus

A Practical Attack on Cyber-infrastructure

University of Colorado
Boulder

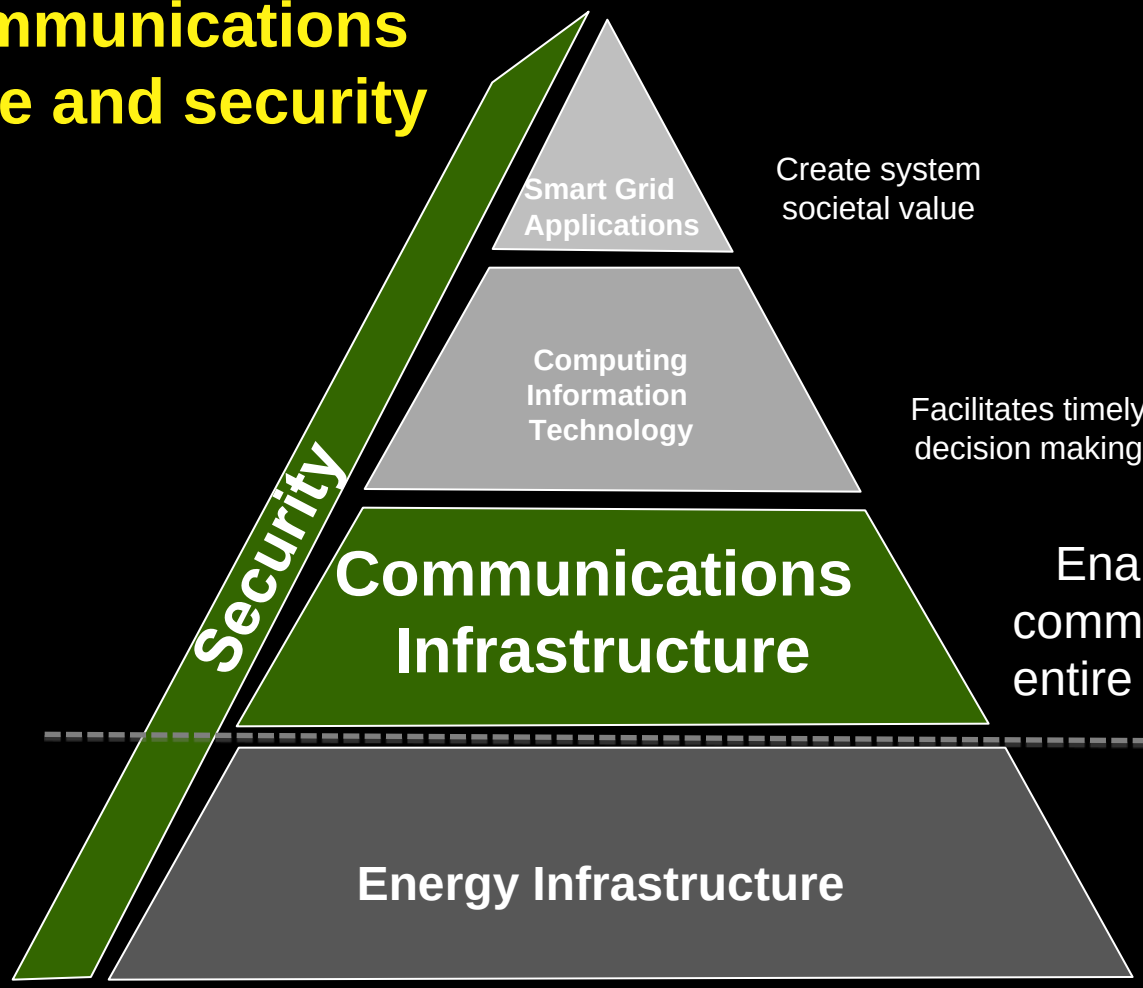
Content

1. **INTRODUCTION**
2. **CRITICAL INFRASTRUCTURE PROTECTION**
   - *History, Agencies, and Standards.*
   - *Cybersecurity for IEC 61850*
   - *The Encryption & Message Authentication vs Latency*
3. **EXPLOITING THE GOOSE PROTOCOL**
   - *Normal GOOSE Function*
   - *Attack Vectors and Techniques*
   - *Attack Consequences*
4. **BUILDING A PRACTICAL CYBER ATTACK**
   - *Technical Details*
   - *Building the Script*
   - *The Results of the Attack*
5. **CONCLUSION**

INTRODUCTION: Digital Energy Program

University of Colorado Boulder

Graduate Education Program on utility communications infrastructure and security



Create system societal value

Facilitates timely decision making

Enables 2-way communications to entire supply chain

Physical structure distributes energy

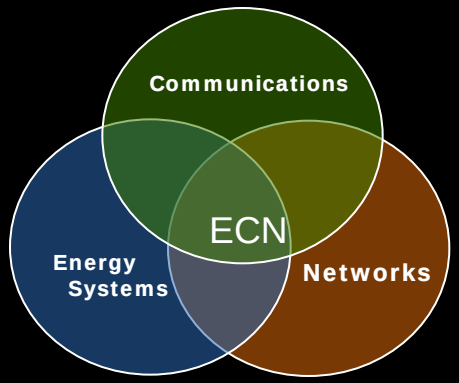
INTRODUCTION: Digital Energy Program

University of Colorado Boulder

Master's Degree

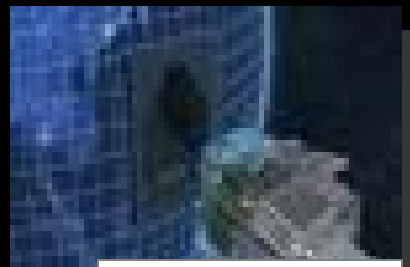
Telecom based-degree and includes essential cross disciplines subjects:

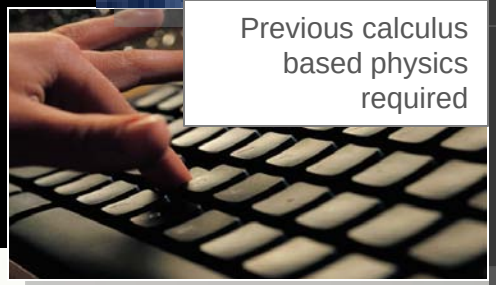
- Technology
- Business and economics
- Regulatory policy



ECN certificate

- Telecommunications Systems
- Data Communications I
- Energy Systems
- Energy Communications Networks

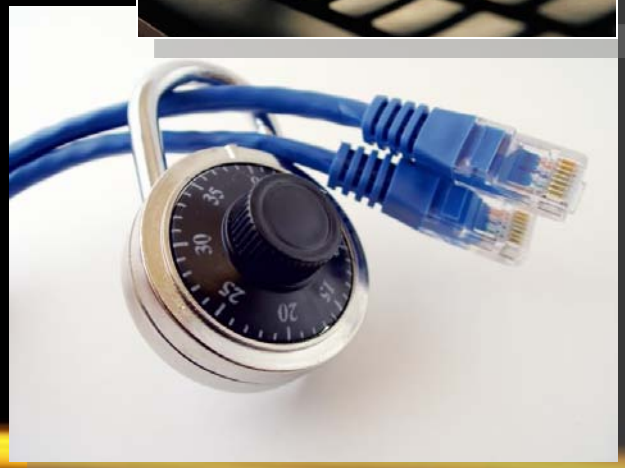




Previous calculus based physics required

Apply the ECN certificate toward your master's degree - add another specialization.

- Power electronics
- Network architecture
- Wireless networks
- Computer and network security
- Project management



INTRODUCTION

CRITICAL INFRASTRUCTURE PROTECTION

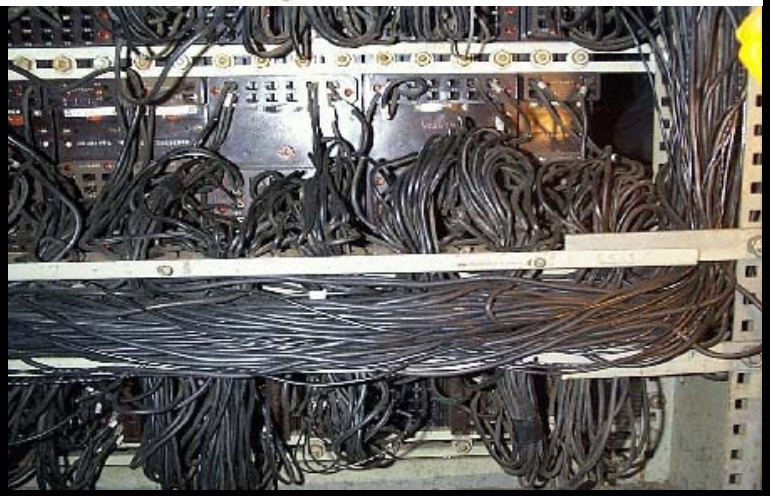
- *History, Agencies, and Standards.*

EXPLOITING THE GOOSE PROTOCOL

- *Attack Consequences*

What is 61850 ?

INTRODUCTION



- **Process Data**
  - Trips, Alarms, interlocking
- **Operational Data.**
  - Status
  - Remote Control
  - Metering
- **Non Operational Data**
  - **Control of Losses**
  - **Asset Management Data**
    - IEDs Management
    - Event Data Collection.

CRITICAL INFRASTRUCTURE PROTECTION

IEC 61850

- **MMS**
  - Status
  - Measurements

Layer 2 or peer to peer communications.

- **GOOSE**
  - Trip
  - Interlocking
  - Status
- **SMV**
  - Measurement for protective functions

IEC 61850 v1 Release 2003

Communication networks and systems in substations

No security for GOOSE message, confined in a physical perimeter

IEC 61850 v2 Release 2008

Communication networks and systems for power utility automation.

12

IEC 61850

13

CRITICAL INFRASTRUCTURE PROTECTION

- *Cybersecurity for IEC 61850*

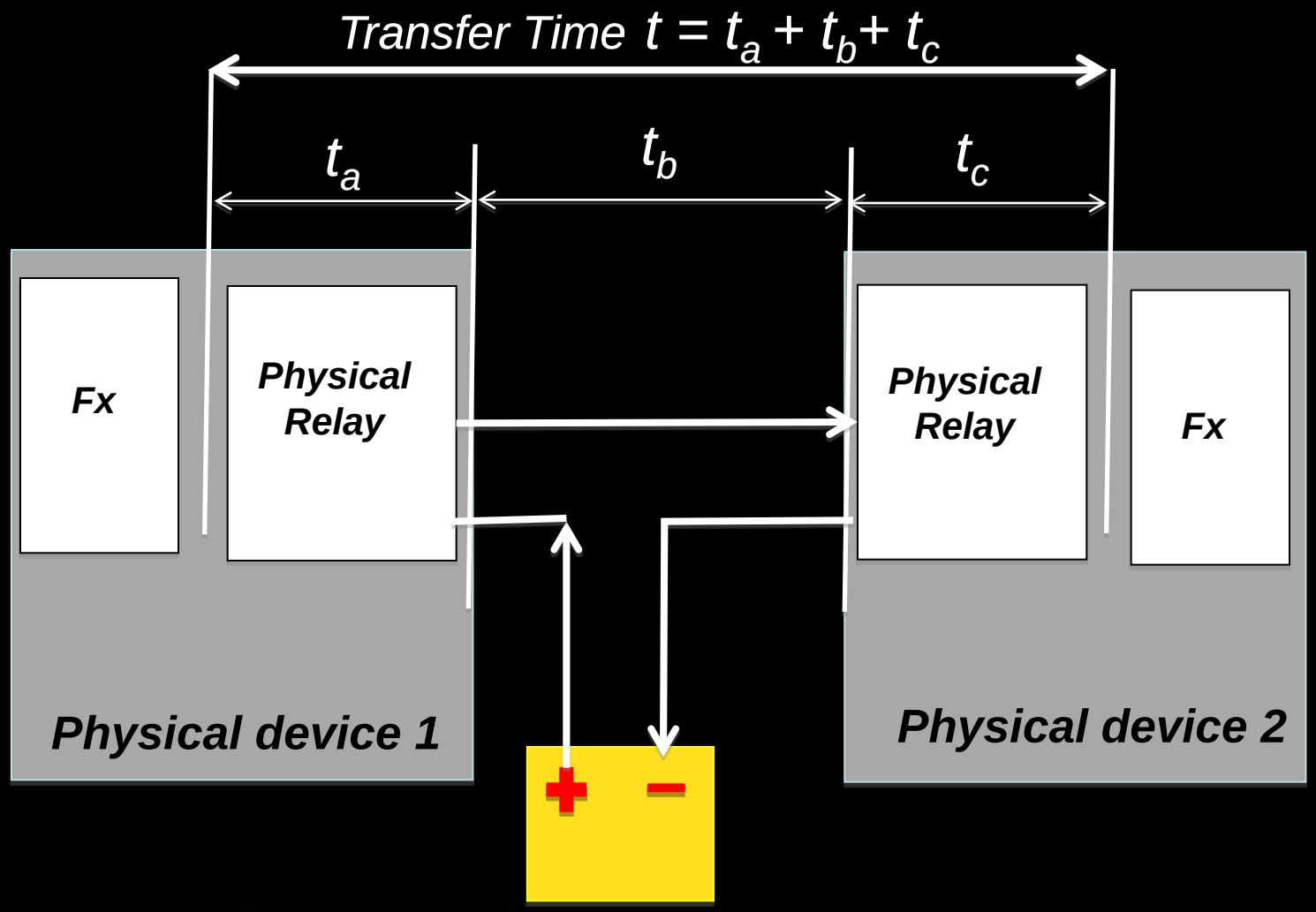
IEC 62351

1. Introduction to the standard
2. Glossary of terms
3. Security for any profiles including TCP/IP,
4. Security for any profiles (MMS, ICCP, IEC 60870-5,)
5. Security for any profiles including (IEC 60870-5, DNP3)
6. Security for IEC 61850 peer to peer profiles
7. Security through network and system management
8. Role-based access control
9. Key Management
10. Security Architecture
11. Security for XML Files

THE ENCRYPTION & MESSAGE AUTHENTICATION VS LATENCY

CRITICAL INFRASTRUCTURE PROTECTION

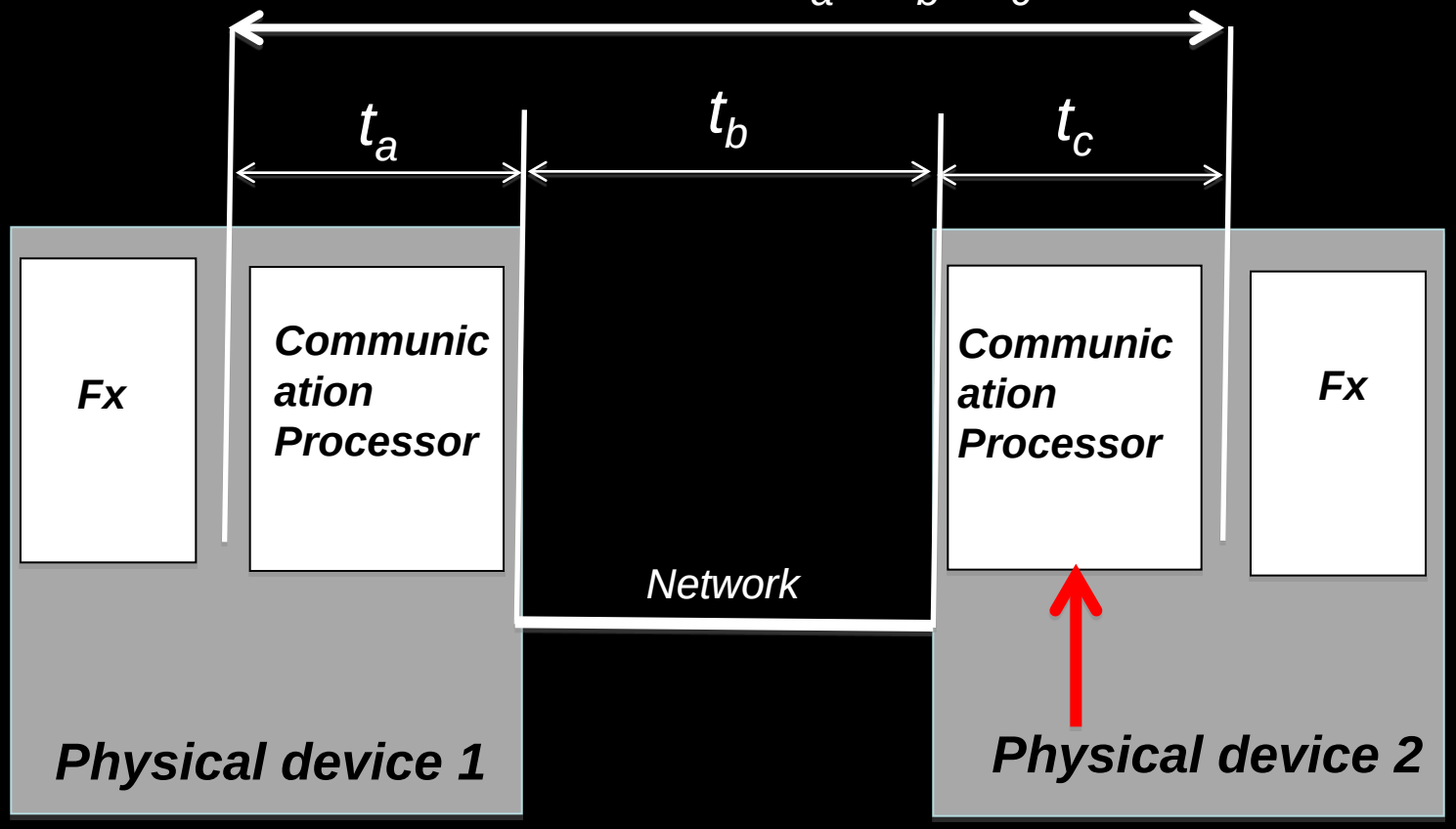
- *The Encryption & Message Authentication vs Latency*



CRITICAL INFRASTRUCTURE PROTECTION

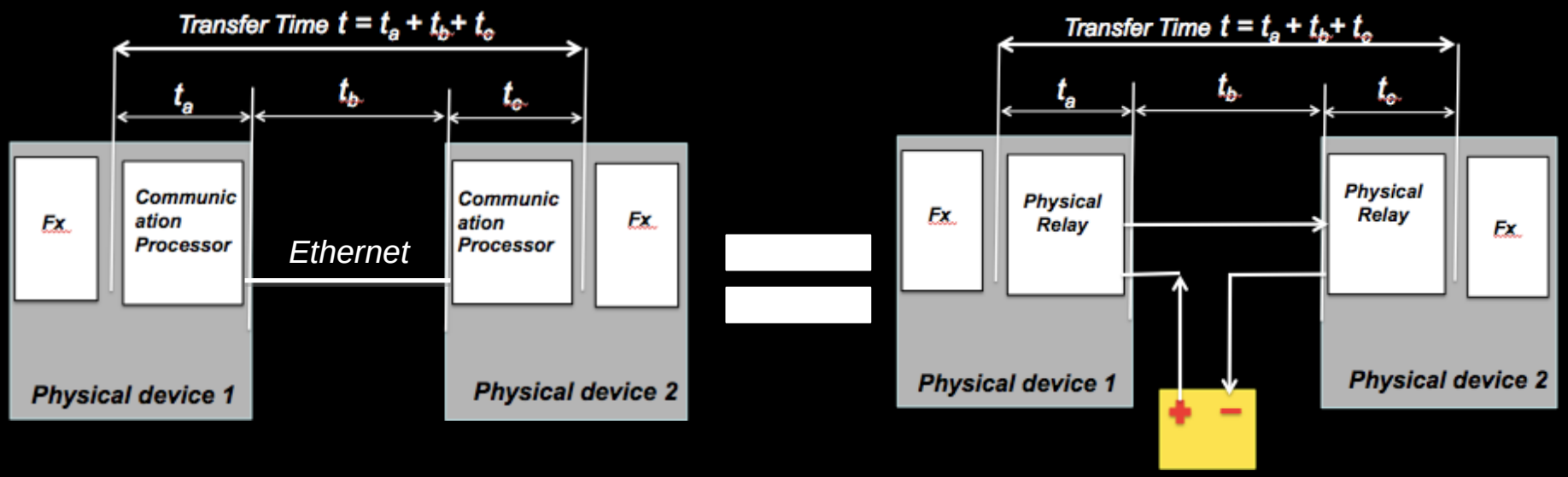
- *The Encryption & Message Authentication vs Latency*

Transfer Time $t = t_a + t_b + t_c$



CRITICAL INFRASTRUCTURE PROTECTION

- *The Encryption & Message Authentication vs Latency*



CRITICAL INFRASTRUCTURE PROTECTION

- *The Encryption & Message Authentication vs Latency*

4ms

CRITICAL INFRASTRUCTURE PROTECTION

- *The Encryption & Message Authentication vs Latency*

Algorithm	Generation Time (ms)	Verification Time (ms)	Bandwidth (bits)
RSA	7.9	0.4	1024
DSA	4.1	4.9	320
ECDSA $F_{2^{160}}$	5.7	7.2	320
ECDSA F_p	4.0	5.2	320
BLS $F_{3^{97}}$	3.5	23.0	170

TIME TO GENERATE AND VERIFY A DIGITAL SIGNATURE ON A 1.0 GHZ PENTIUM III PROCESSOR FOR DIFFERENT SCHEMES

CRITICAL INFRASTRUCTURE PROTECTION

- *The Encryption & Message Authentication vs Latency*

Digital Signature Generation	**80 bits of security strength:** RSA: $1024 \leq \lvert n \rvert < 2048$ EC: $160 \leq \lvert n \rvert < 224$	Acceptable through 2010 Deprecated from 2011 through 2013 Disallowed after 2013
	≥ 112 bits of security RSA: $\lvert n \rvert \geq 2048$ EC: $\lvert n \rvert \geq 224$	Acceptable
Digital Signature Verification	**80 bits of security strength:** RSA: $1024 \leq \lvert n \rvert < 2048$ EC: $160 \leq \lvert n \rvert < 224$	Acceptable through 2010 Legacy-use after 2010

NIST Special Publication 800-131A

CRITICAL INFRASTRUCTURE PROTECTION

Options

- Install faster processor in the IEDs
- Use processor with embedded security
- Use co-processors ASICs
- Use group-key and certificates

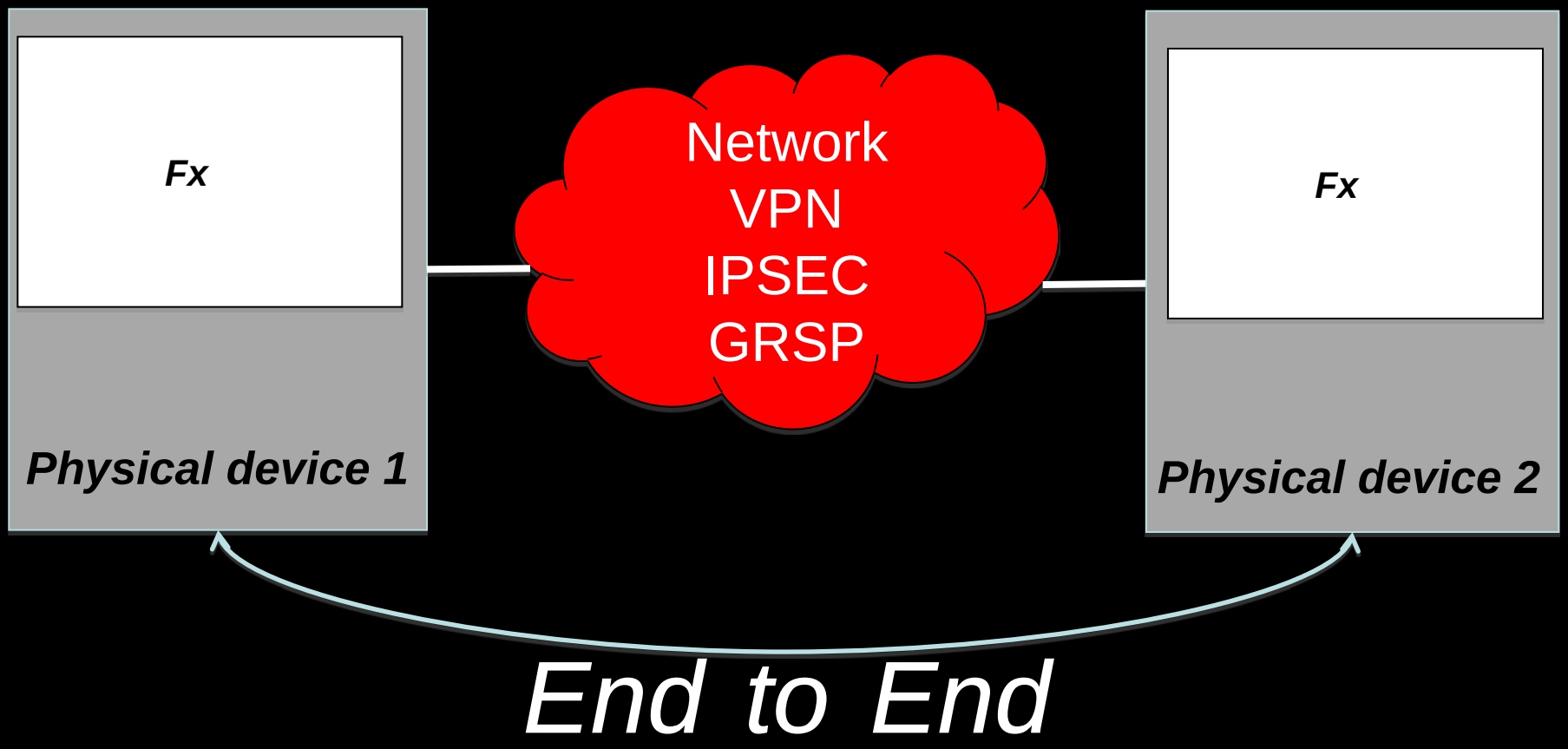
Constrains

- IEDs enclosure, fan-less boxes to avoid dust and bugs
- Limited processor power
- Long life time of IEDs ~10 years
- Backward compatibility
- Who will handle the certificates
- Price-Benefits

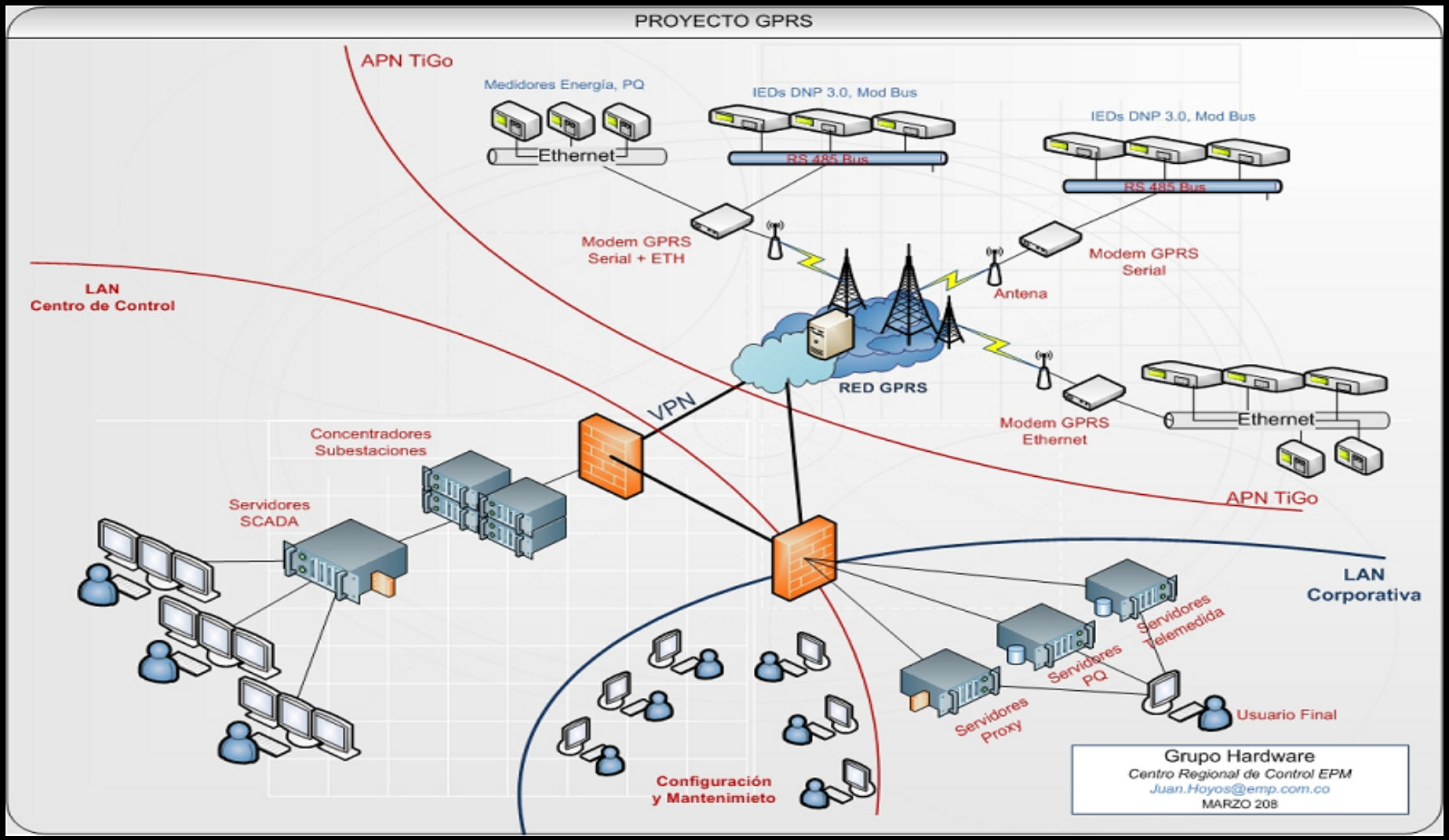
CRITICAL INFRASTRUCTURE PROTECTION

EXPLOITING THE GOOSE PROTOCOL

EXPLOITING THE GOOSE PROTOCOL

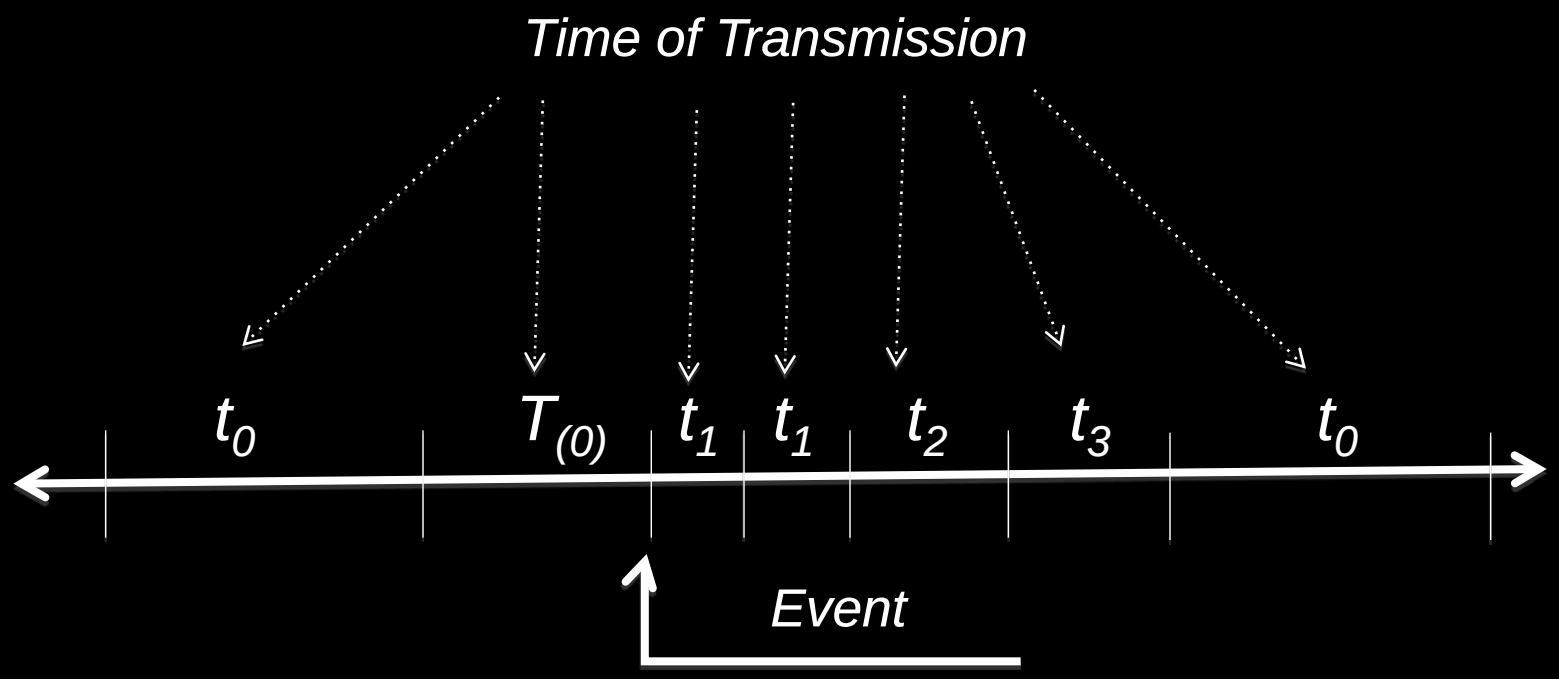


EXPLOITING THE GOOSE PROTOCOL



EXPLOITING THE GOOSE PROTOCOL

- *Normal GOOSE Function*



T_0 Retransmission in stable conditions (no events for long time)
$T_{(0)}$ Retransmission in stable conditions may be shorter by event
T_1 Shortest retransmission time after the event
T_1 T_1 Retransmission time until achieving the stable condition time

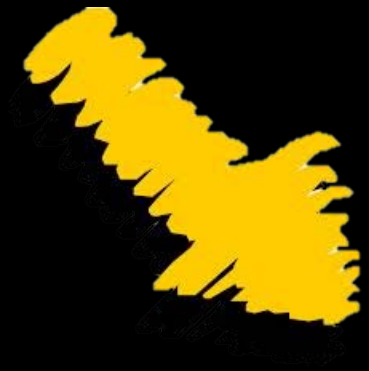
EXPLOITING THE GOOSE PROTOCOL

- *Vulnerabilities*

1. Computer software:
2. Communications links and networking: Communications channel penetration, Network sniffing, Hijacking, Spoofing and playback, Man-in-the-Middle attacks, Denial-of-Service attacks, Internet-related attacks
3. System Administration
4. On employees
5. Miscellaneous

EXPLOITING THE GOOSE PROTOCOL

- *Attack Vectors and Techniques*



EXPLOITING THE GOOSE PROTOCOL

- *Motivations*

EXPLOITING THE GOOSE PROTOCOL

- *Attack Consequences*

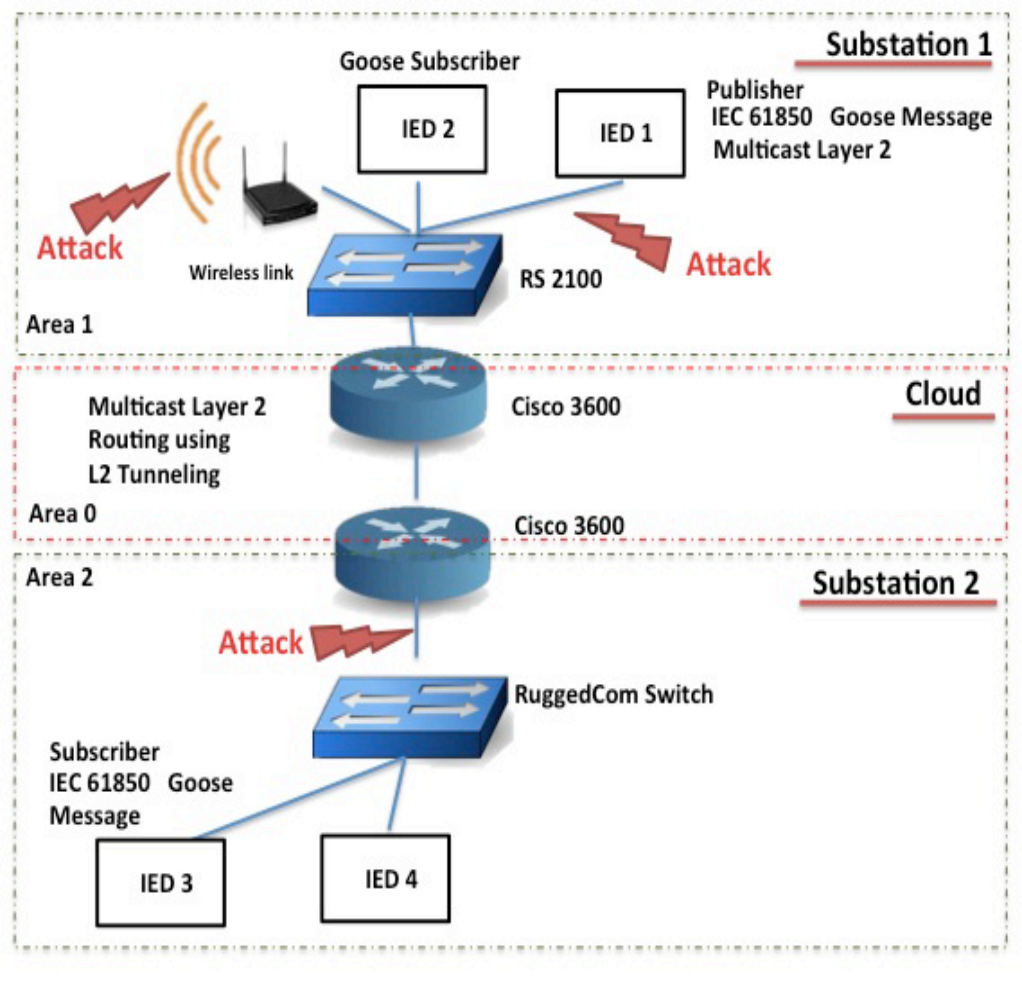
BUILDING A PRACTICAL CYBER ATTACK

- *Technical Details*

1. Identify GOOSE messages in the network Ether-type, 0x88B8.
2. Decode the GOOSE message using the definition of ASN1 described in the IEC 61850-8-1.
3. Look for three specific fields: stNum, sqNum, and the Boolean values inside the data sets
4. Change the data for any Boolean value inside the data-set, if the value is true the code overwrites a false and vice versa.
5. Generate the spoofed messages
6. Send them through the network with the same source and destination MAC address as the valid user.

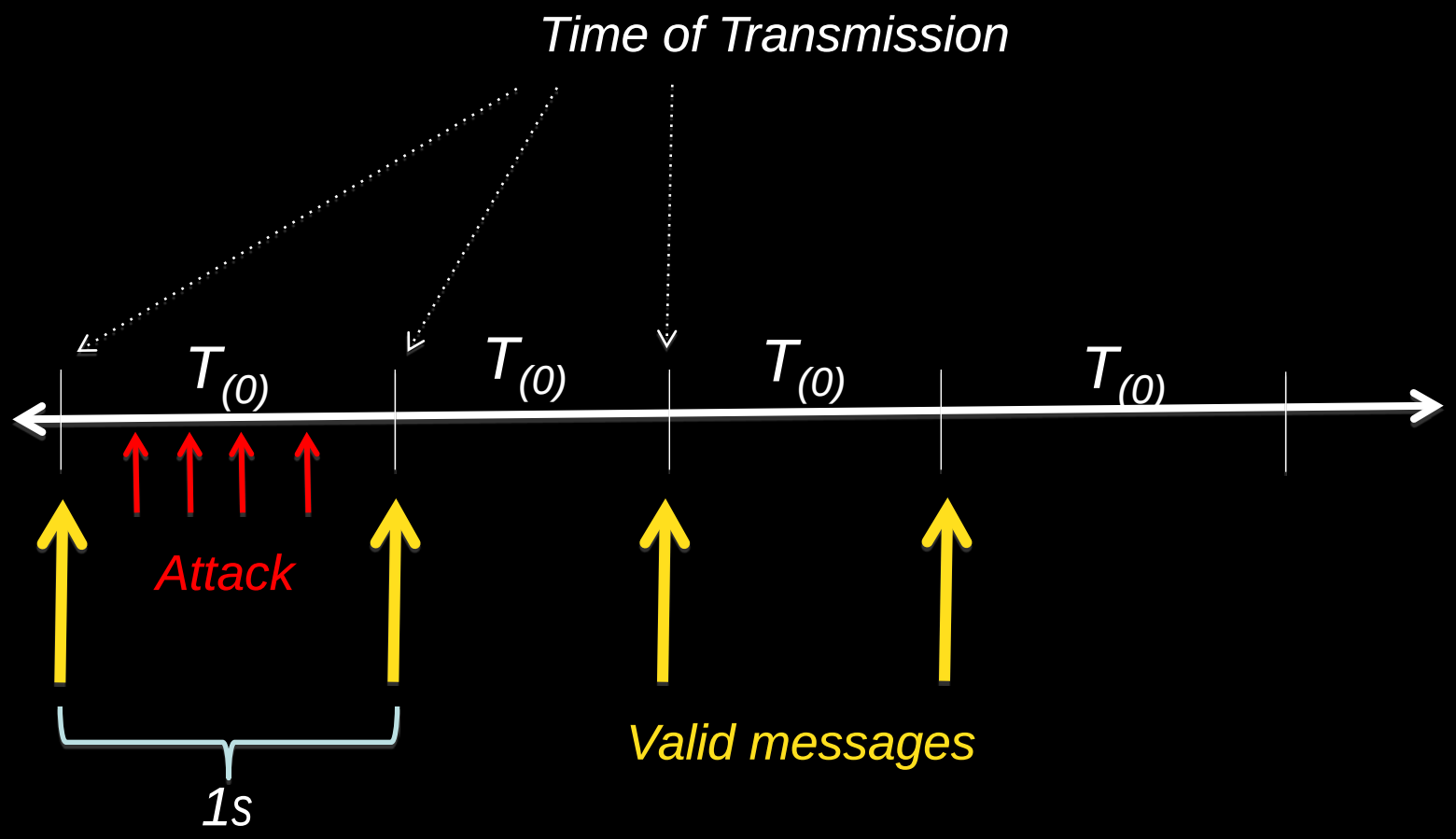
BUILDING A PRACTICAL CYBER ATTACK

- (2) Cisco 3600 Routers
- (1) RuggedCom 2100
- (1) RuggedCom RS900
- (1) Linksys wireless router
- (4) IEDs.
- (1) MacBook Air 1.5Ghz Intel core i5



BUILDING A PRACTICAL CYBER ATTACK

- *Building the Script*



BUILDING A PRACTICAL CYBER ATTACK

- *The Results of the Attack*

193	107.246091		00:47:d0	Iec-Tc57_01:00:03	GOOSE	143
194	107.246624		00:47:d0	Iec-Tc57_01:00:03	GOOSE	143
195	107.247129		00:47:d0	Iec-Tc57_01:00:03	GOOSE	143
196	107.247950		00:47:d0	Iec-Tc57_01:00:03	GOOSE	143
197	107.249885		00:47:d0	Iec-Tc57_01:00:03	GOOSE	143
198	108.243873		00:47:d0	Iec-Tc57_01:00:03	GOOSE	144

Same MAC source

4	06/13/12	18:24:09.637	OUT101	Deasserted
3	06/13/12	18:24:09.642	OUT101	Asserted
2	06/13/12	18:24:10.637	OUT101	Deasserted

CONCLUSION

CONCLUSION