Security for the Industrial Internet of Things (IIoT)

Class 4: Data Theft and Attacks

September 20, 2018

Louis W. Giokas

Presented by:

DesignNews

CEC CONTINUING EDUCATION CENTER

Digi-Key ELECTRONICS

This Week's Agenda

Monday	IIoT Landscape
Tuesday	Safety Considerations
Wednesday	Security Concerns
Thursday	Data Theft and Attacks
Friday	Solutions and Future Directions

Course Description

As the Industrial Internet of Things (IIoT) expands into ever more areas, issues with security become critical. Some of the greatest benefits to be gained come from connecting systems and sensors on the factory floor to corporate systems and multiple sites. The downside is that this leaves these systems, which are critical to the business, open to intrusions, potentially negating the benefits. There are two areas of vulnerability. The first is disruption of operations. The second is the theft of data. In this course, we will look at some of the issues involved and potential solutions to both problems. These include some standard solutions to protect infrastructure as well as solutions that can be embedded in the protocol stack of the devices themselves.

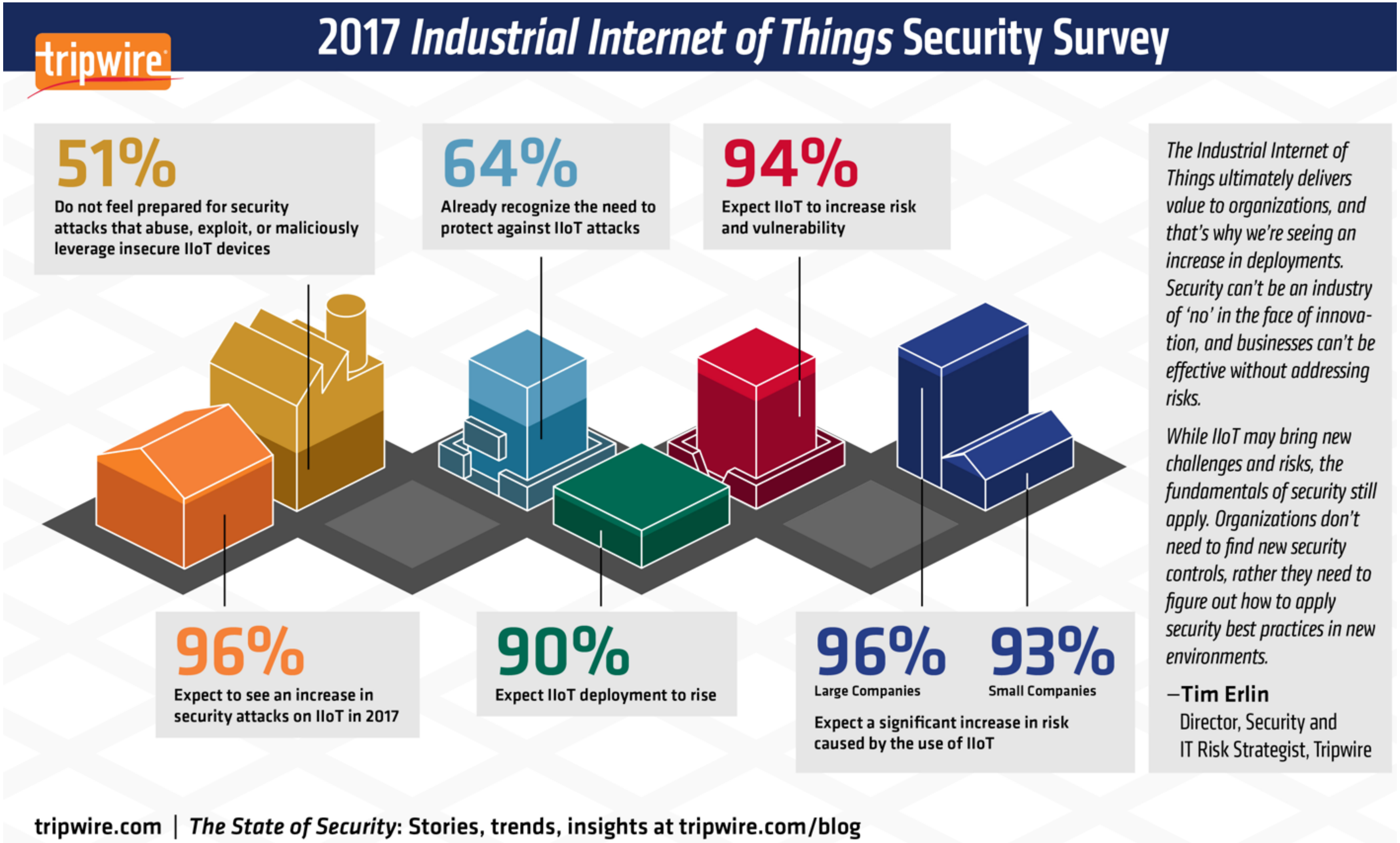
Today’s Agenda

- Overview
- Data Types
- Privacy Concerns
- Threat Vectors
- Attack Types
- Conclusion/Next Class

Overview

- Data is at the heart of any industrial enterprise today
  - We use it to design, develop, manufacture and market our products
- Data is fast becoming an asset in its own right
- Protection of data is a critical function in the enterprise
  - Failure to do so has drastic consequences

Overview



2017 *Industrial Internet of Things* Security Survey

51%
Do not feel prepared for security attacks that abuse, exploit, or maliciously leverage insecure IIoT devices

64%
Already recognize the need to protect against IIoT attacks

94%
Expect IIoT to increase risk and vulnerability

96%
Expect to see an increase in security attacks on IIoT in 2017

90%
Expect IIoT deployment to rise

96%
Large Companies

93%
Small Companies

Expect a significant increase in risk caused by the use of IIoT

The Industrial Internet of Things ultimately delivers value to organizations, and that's why we're seeing an increase in deployments. Security can't be an industry of 'no' in the face of innovation, and businesses can't be effective without addressing risks.

While IIoT may bring new challenges and risks, the fundamentals of security still apply. Organizations don't need to find new security controls, rather they need to figure out how to apply security best practices in new environments.

—**Tim Erlin**
Director, Security and
IT Risk Strategist, Tripwire

tripwire.com | *The State of Security*: Stories, trends, insights at tripwire.com/blog

Overview

- Protection of data in corporate systems is well developed
  - Even so, there have been breaches in those systems
- IIoT extends the attack surface considerably
  - This one, as we have seen, is much harder to harden
  - This translates to many more threat vectors
  - Can also extend up into the corporate systems

Overview

- Loss, or theft, of critical corporate data in the IIoT setting can lead to a number of consequences and costs
  - – Financial
    - Costs to reconstitute, recover data
    - Costs of business disruption
  - – Intellectual Property
    - Loss of business
  - – General business and reputational disruption

Data Types

- The highly networked systems we have been considering hold data at many levels
  - Operational data
  - Control data
  - Engineering data
    - Designs
    - IIoT system models
- Financial data is handled in corporate systems and protected separately
  - But, there can be networked connections

Data Types

- One way of characterizing data generated by the IoT, and therefore IIoT, is the following:
  - Status
  - Location
  - Automation
  - Actionable (status data that triggers and action)
- In industrial settings there are two major differences
  - Complexity (i.e., vision data)
  - Timing constraints

Data Types

- Data can also be characterized by how it is used
  - Control
    - Real-time
  - Measurement
  - Analytical
  - Engineering
- These have different characteristics and value to an attacker

Privacy Concerns

- Privacy is one of the important areas of concern in the IIoT
  - Sensitive corporate data must be protected
  - Customer, or customer related, information can be compromised
  - Increased exposure of corporate networks
  - Reliance of the corporation on data
- This has become a boardroom issue
  - Cyber resilience is the term often used

Privacy Concerns

- Attackers can comprise data in an IIoT in a number of ways
  - Basic theft: leaves the data intact, but it is now in the hands of the attacker
  - Ransom: actual takeover of a system’s data
  - Corruption: potentially cause damage in the plant
- Detection of some of these is not always possible and impact not always direct

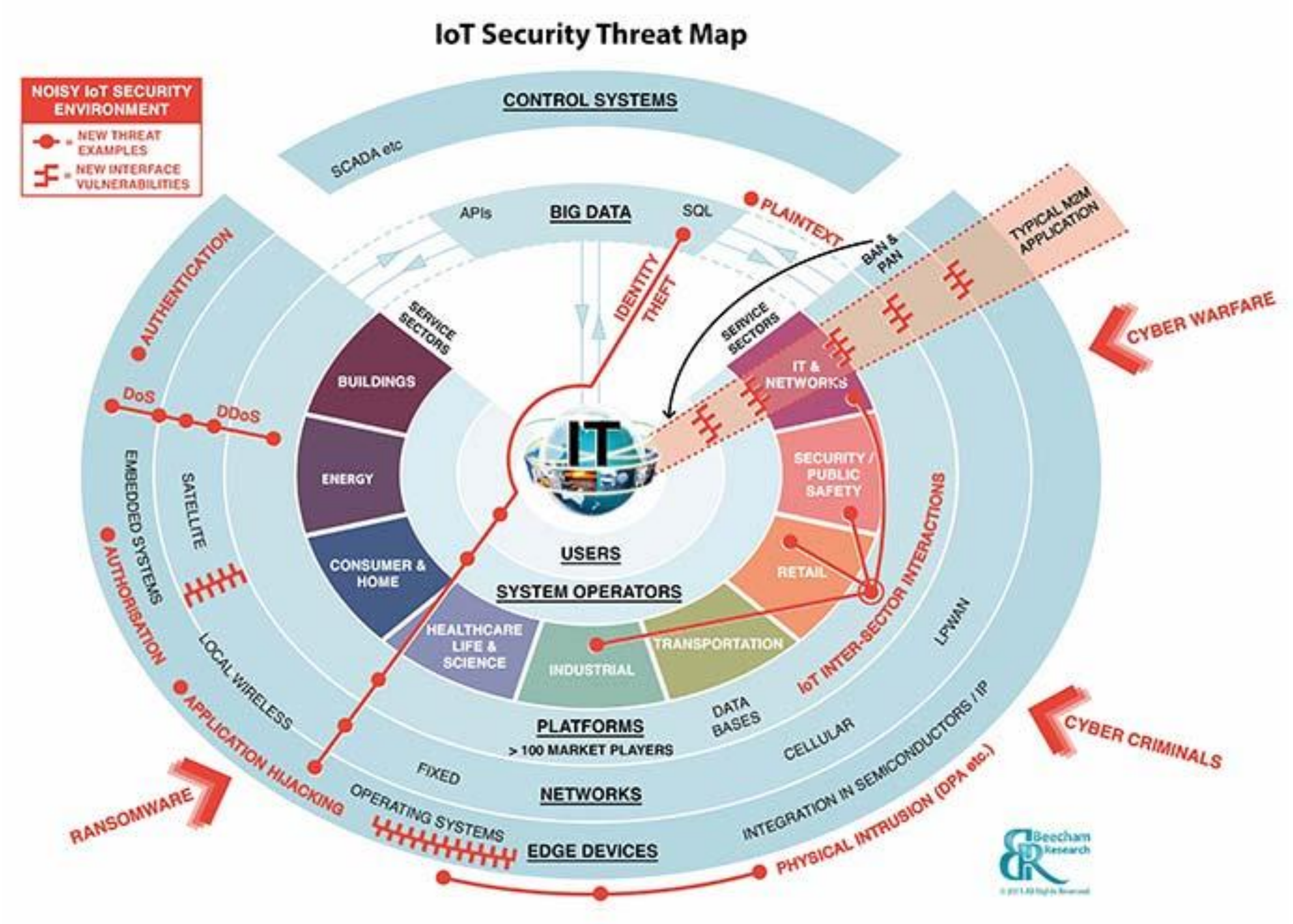
Threat Vectors

- By "threat vectors" we mean the ways in which an attacker may get access to a system
- The goal of that access may be to plant malware or to steal data
- Points of entry into the IIoT are many and varied
  - Not all result in major breaches
    - E.g., a logistics system will not be directly connected to the factory floor, it will go through the ERP system which provides additional isolation

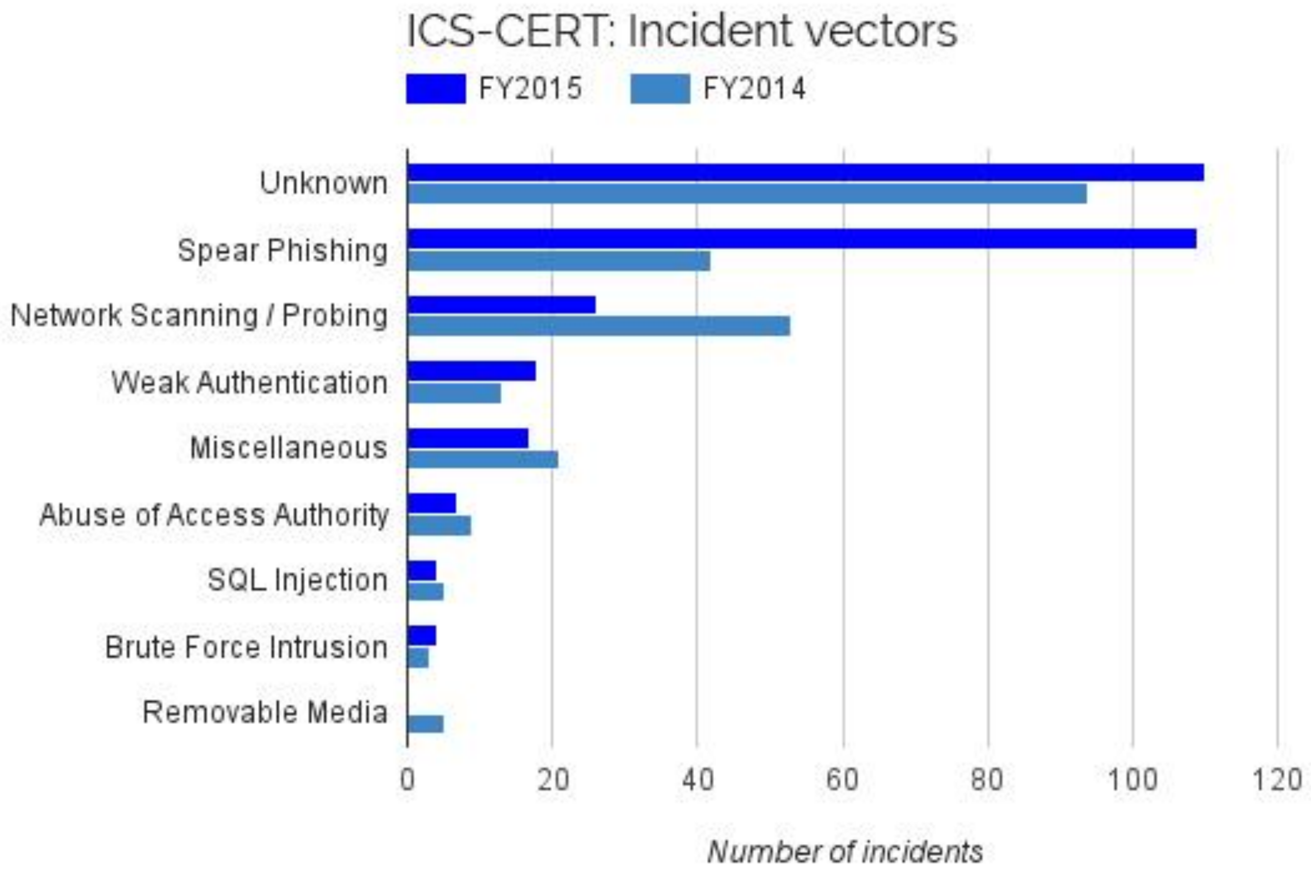
Threat Vectors

- Many attacks come through the corporate systems that are connected to the Internet
  - Easiest point of entry
- In-plant attacks are difficult because it is possible to provide physical security
  - Threat vector here is an employee or someone authorized to be in the plant

Threat Vectors



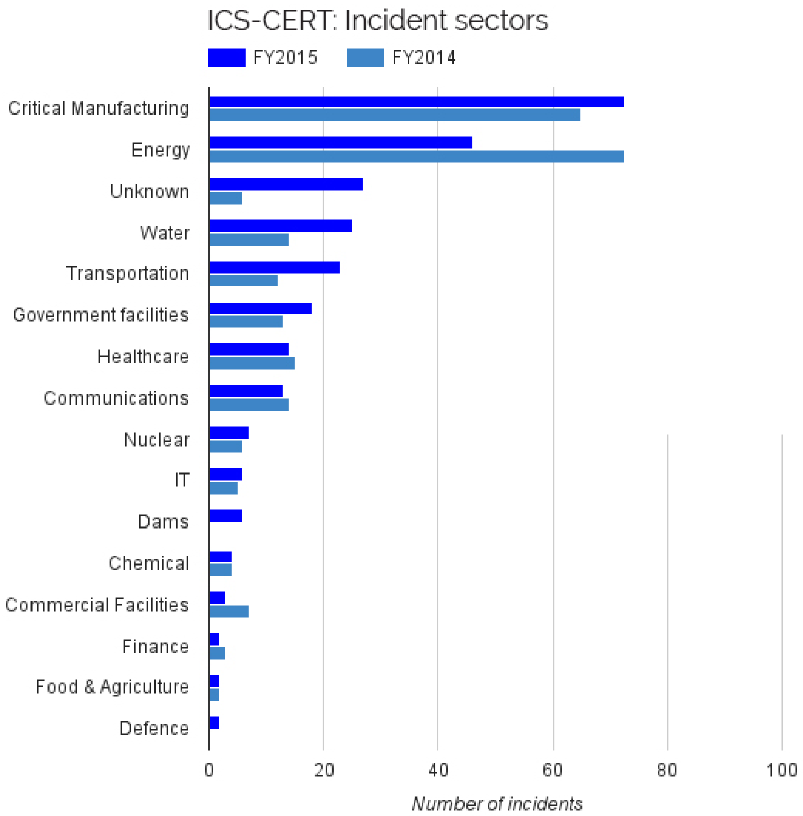
Attack Types

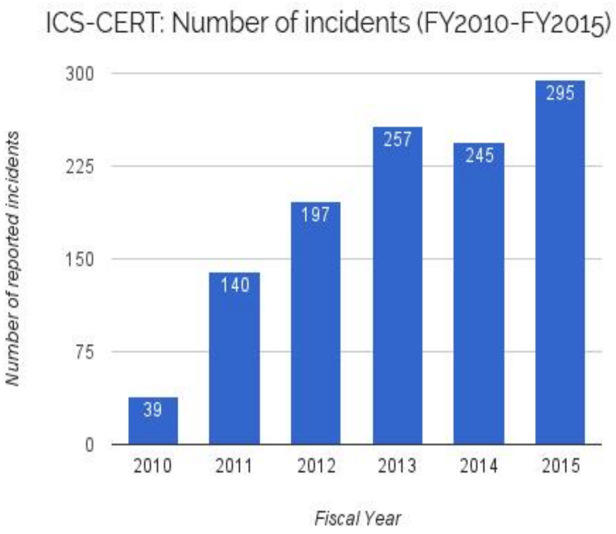


Attack Types

- Attacks can range from DDoS to data theft to system disruption
- There is an organization that responds to these, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
  - They have classified and quantified the threat landscape

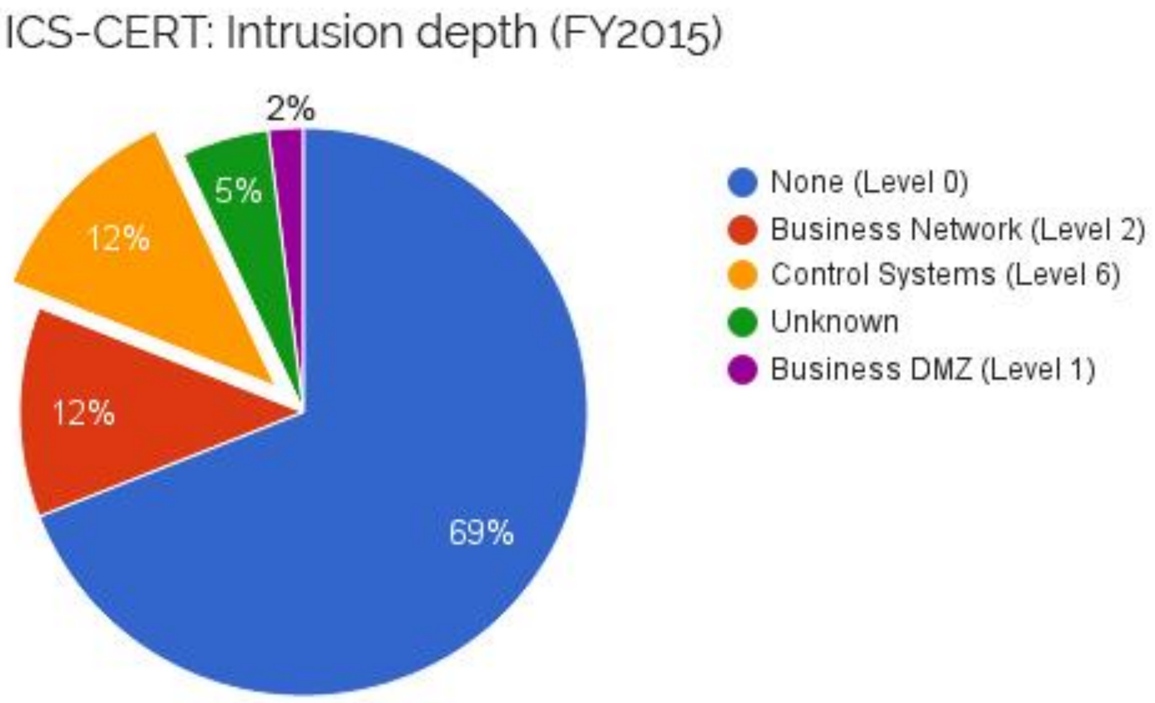
Attack Types





Quantification of the threat

Attack Types



Conclusion/Next Class

- In this session we have concentrated on the aspects of data security
  - We have covered theft and attack issues
- The magnitude of the problem is growing
- Tomorrow we will discuss some strategies that may help combat the threats