What is security?

Enforcing a desired property ***in the presence of an attacker***

data confidentiality

user privacy

data and computation integrity

authentication

availability

…

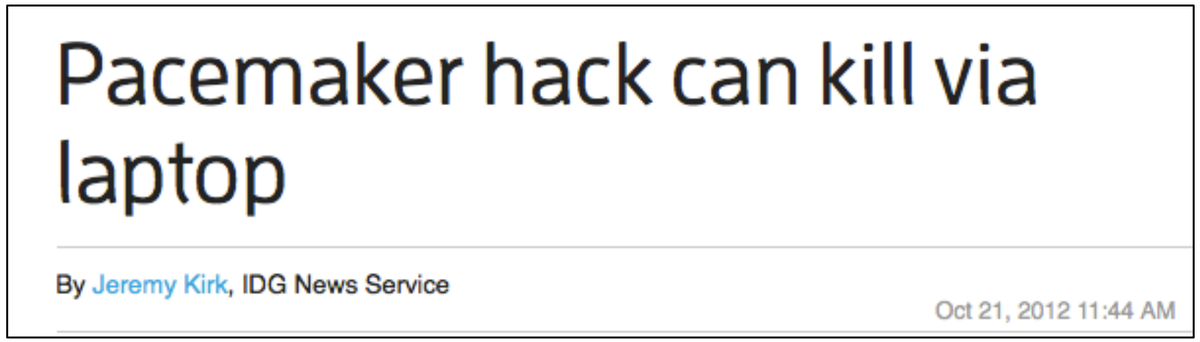
Today's outline

- Why is security important?
- Course logistics
- Intro to security principles

Why is security important?

- It is important for our
  - physical safety
  - confidentiality/privacy
  - functionality
  - protecting our assets
  - successful business
  - a country's economy and safety
  - and so on…

Physical safety threats



Pacemaker hack can kill via laptop

By Jeremy Kirk, IDG News Service

Oct 21, 2012 11:44 AM

Business

FBI probe of alleged plane hack sparks worries over flight safety

Privacy/confidentiality

91% OF HEALTHCARE ORGANIZATIONS HAVE REPORTED A DATA BREACH IN THE LAST FIVE YEARS.

By elxradmin Posted May 29, 2015 In health IT, security

EVERYDAY MONEY IDENTITY THEFT

Data Breach Tracker: All the Major Companies That Have Been Hacked

Breaches in 2015 [ITRC]:

- Number of breaches = 5,497
- Number of Records = 818,004,561

Can affect a country's economy... Multiple times!

KIM ZETTER SECURITY 03.03.16 7:00 AM

INSIDE THE CUN UNPRECEDENTE UKRAINE'S POW

A Cyber-Weapon Warhead Test

By **Nicholas Weaver** Wednesday, June 14, 2017, 11:38 AM

The *Daily Beast* has a story on "CrashOverride", a computer program best described as transient anti-infrastructure warhead designed to disrupt the power grid. It was tested live against a Ukrainian substation in December 2016 creating a small blackout. Kim Zetter has another good report at *Motherboard*, and Dragos has the technical details.

Dragos attributes the attack as conducted by "ELECTRUM", a group it assesses as being associated with Sandworm—an evaluation that is only slightly better than rolling attribution dice. It is probably more accurate to phrase the attribution as "probably Russia, and probably affiliated with the previous Ukrainian power grid attack in 2015." (The December 2016 attack was the second assault on the Ukranian

een ion he en to nat ers.

And It Is National Security!

THE WALL STREET JOURNAL.

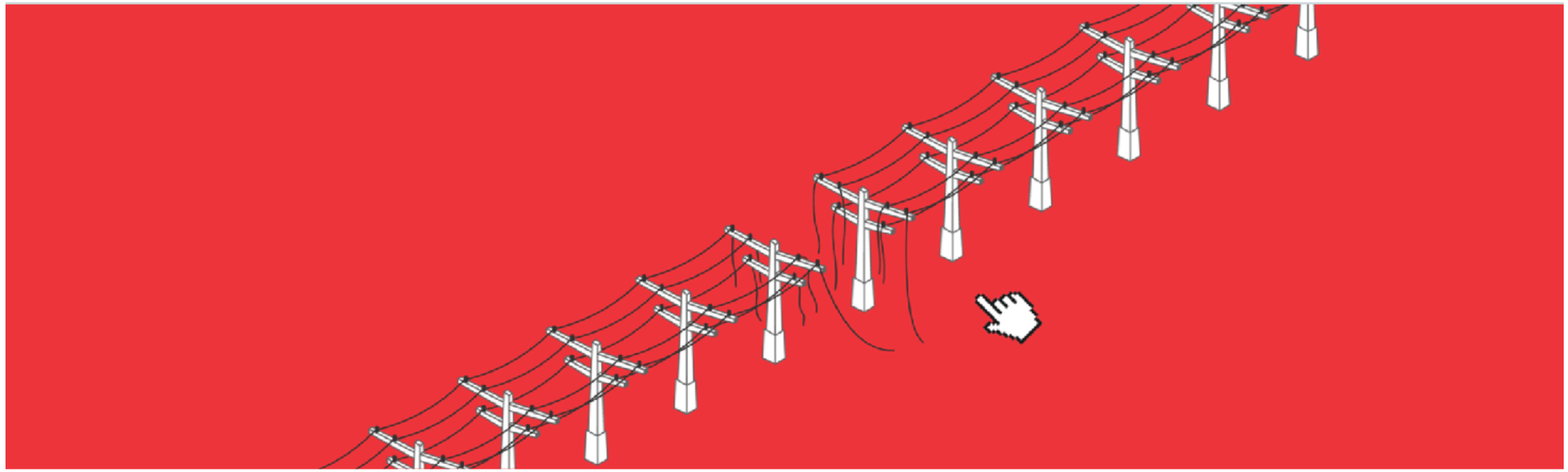


ILLUSTRATION BY JESSICA KURONEN/WSJ

America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It

A Wall Street Journal reconstruction of the worst known hack into the nation's power system reveals attacks on hundreds of small contractors

And NotPetya...

- Attackers compromised the update channel for MeDoc
  - Think "TurboTax For Business in Ukraine":
    One of only two accounting packages which Ukrainian businesses can use to pay taxes
- They then monitored for weeks with their backdoor
  - This gave them a foothold in almost all who have business
- Then they released a malicious "worm
  - It spread from computer to computer, and then with a fake "ransomware" payload
    - This cost Mersk shipping alone ***$100M-300M*** in lost r
      White House estimates $10B in damage

SECURITY 08.22.18 05:00 AM

THE UNTOLD STORY OF NOTPETYA, THE MOST DEVASTATING CYBERATTACK IN HISTORY

Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world.

BY ANDY GREENBERG

IT WAS A perfect sunny summer afternoon in Copenhagen when the world's largest shipping conglomerate began to lose its mind.

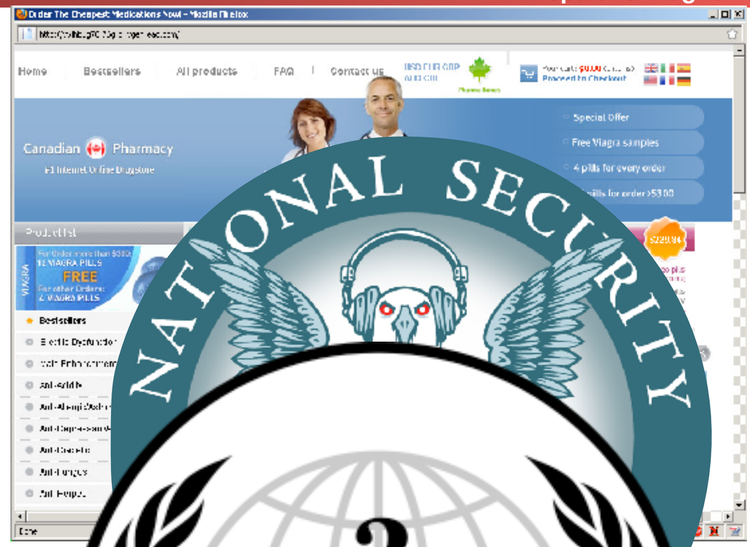
The headquarters of A.P. Møller-Maersk sits beside the breezy

Security Principles

- People and Money
- Threat Model
- Prevention, Detection & Response, Mitigation and Recovery
- False Positives, False Negatives, and Compositions

It All Comes Down To People... The Attacker(s)

- People attack systems for some reason
  - They may do it for money
  - They may do it for politics
  - They may do it for the lulz
  - They may just want to watch the world burn
- Often the most effective security is to attack the attacker's motivation



Personal Security: Threat Model...

- Who and why might someone attack ***you***?
- Criminals for money
- Teenagers for laughs or to win in an online game
- Governments
  - Probably not: We aren't important enough
  - And even if important enough we're only worth the B game: aka the same things used against us by criminals
- Intimate partners

It All Comes Down to People... The Users

- If a security system is unusable it will be unused
  - Or at least so greatly resented that users will actively attempt to subvert it:
    "Let's set the nuclear launch code to 00000000!"
    (oh, and write down the password anyway!)
- Users will subvert systems anyway
- Programmers will make mistakes
- And Social Engineering...