On Security Issues

Carl Landwehr
NSF

Autonomic Web Computing - Security

1. What kinds of attacks are prevalent today and what kinds are expected in the future?

2. What techniques are currently available to defend e-commerce sites against these attacks?

3. How are security configurations for web services specified, configured, and verified? To what extent can these functions be automated?

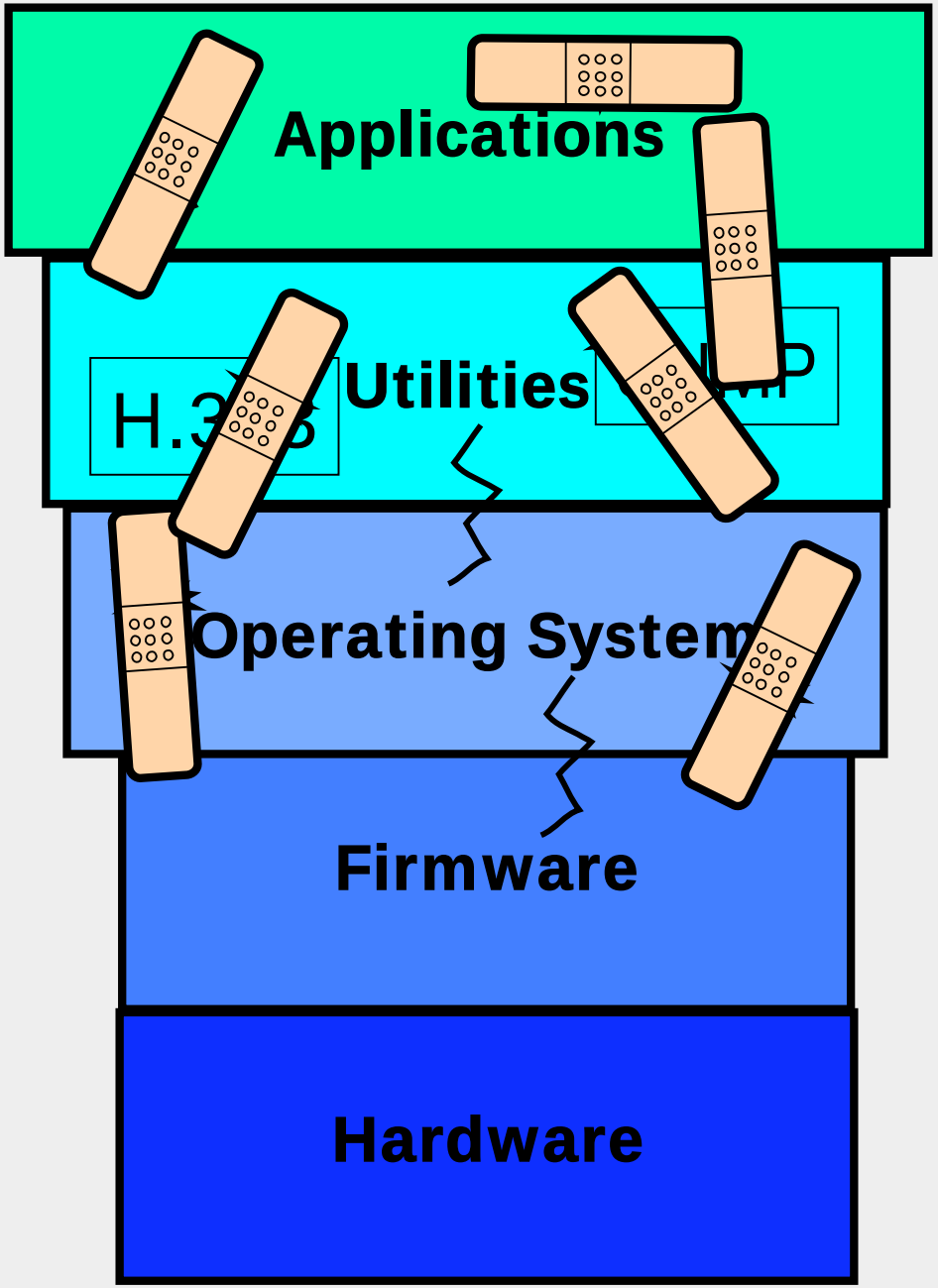
4. What is the distance between theory (e.g. in cryptographic protections) and mechanisms actually in use?

Brian L
&
Bob B

Elisa B
&
Sanjain N

John B

Autonomic Security?



We built it – can we fix it?

- How must it be?
  - What are the limits?
- How might it be?
  - What are the possibilities

Some Limits

- Mathematical/logical
  - Access control questions in some models are undecidable (HRU, 1976)
  - Obfuscation is impossible (BGIRSVY, 2001)
  - One time pads can support unbreakable ciphers
  - Shannon's theorem bounds channel capacity
- Physical
  - Reading a quantum-entangled photon alters its state
  - The speed of light limits the rate of information transmission
- Economic
  - Rational consumers don't spend money on undetectable properties
- Social
  - Perfection is not of this world

Observation: the economic and social limits have limited security more than the mathematical and physical ones

Some Current Assumptions

- Internet protocols can't be substantially changed or replaced
- Operating systems will have 50 million lines of code or more
- Security must be reactive

We need to think further out

- **Couldn't we at least:**
  - Create and deploy mechanisms to allow us to identify where a message originated with a good degree of certainty
  - Figure out how to build system interfaces that real people (users and developers) can understand and use
  - Learn how to organize systems so that even when imperfect, they are not prone to catastrophic failure under attack

We are a long way from the limits

We need to think of more possibilities

Discussion?