Laws of Cyber Security

Ravi Sandhu
Executive Director and Endowed Professor
September 2010

ravi.sandhu@utsa.edu, www.profsandhu.com, www.ics.utsa.edu

Microsec vs Macrosec

From Wikipedia, the free encyclopedia:

Microeconomics (from Greek prefix micro- meaning "small" + "economics") is a branch of economics that studies how the individual parts of the economy, the household and the firms, make decisions to allocate limited resources, typically in markets where goods or services are being bought and sold. Microeconomics examines how these decisions and behaviors affect the supply and demand for goods and services, which determines prices, and how prices, in turn, determine the supply and demand of goods and services.

This is a contrast to **macroeconomics**, which involves the "sum total of economic activity, dealing with the issues of growth, inflation, and unemployment. Microeconomics also deals with the effects of national economic policies (such as changing taxation levels) on the before mentioned aspects of the economy.

- Retail Attacks
- Targeted Attacks

Microsec

- 99% of the attacks are thwarted by basic hygiene and some luck
- 1% of the attacks are difficult and expensive, even impossible, to defend or detect

IP Spoofing Story

- IP Spoofing predicted in Bell Labs report ≈ 1985
- 1st Generation firewalls deployed ≈ 1992
- IP Spoofing attacks proliferate in the wild ≈ 1993
- VPNs emerge ≈ late 1990's
- Vulnerability shifts to accessing end-point
- Network Admission Control ≈ 2000's

Evolution of Phishing

- Phishing 1.0
  - Attack: Capture reusable passwords
  - Defense: user education, cookies, pictures
- Phishing 2.0
  - Attack: MITM in the 1-way SSL channel, breaks OTPs
  - Defense: 2-way SSL
- Phishing 3.0
  - Attack: Browser-based MITM client in front of 2-way SSL
  - Defense: Transaction authentication outside browser
- Phishing 4.0
  - Attack: PC-based MITM client in front of 2-way SSL
  - Defense: Transaction authentication outside PC, PC hardening

Sandhu's Laws of Attackers

1. Attackers exist
   - You will be attacked
2. Attackers have sharply escalating incentive
   - Money, terrorism, warfare, espionage, sabotage, …
3. Attackers are lazy (follow path of least resistance)
   - Attacks will escalate BUT no faster than necessary
4. Attackers are innovative (and stealthy)
   - Eventually all feasible attacks will manifest
5. Attackers are copycats
   - Known attacks will proliferate widely
6. Attackers have asymmetrical advantage
   - Need one point of failure

Operational Principles

A. Prepare for tomorrow's attacks, not just yesterday's
   - Good defenders strive to stay ahead of the curve, bad defenders forever lag

B. Take care of tomorrow's attacks before next year's attacks
   - Researchers will and should pursue defense against attacks that will manifest far in the future BUT these solutions will deploy only as attacks catch up

C. Use future-proof barriers
   - Defenders need a roadmap and need to make adjustments

D. It's all about trade-offs
   - Security, Convenience, Cost

Macrosec

- Rational microsec behavior can result in highly vulnerable macrosec