# Attack Resistance Score

taking the high, medium and low out of risk analysis

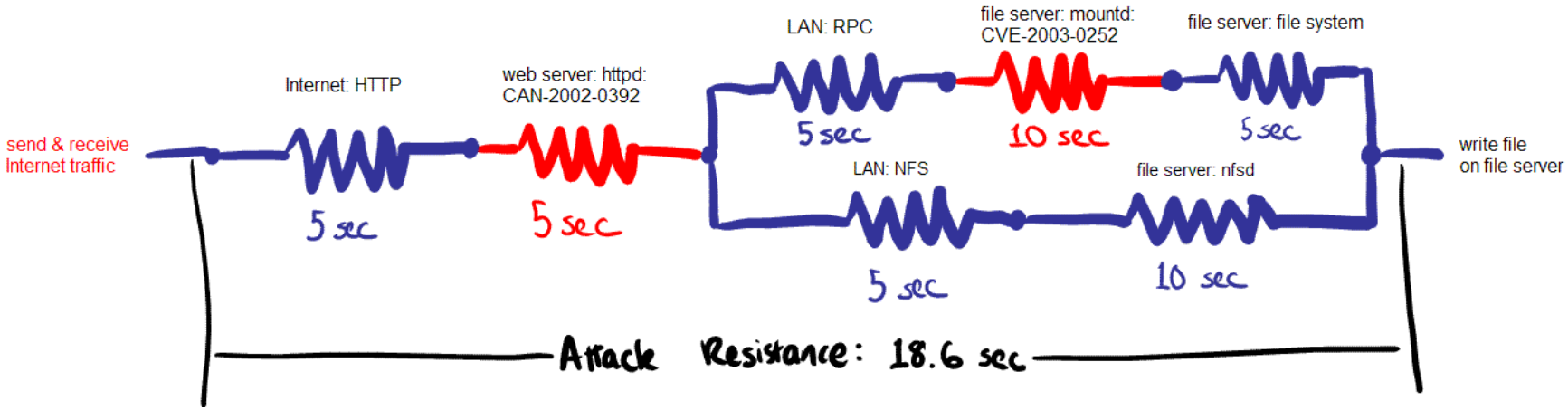

Brenda Larcom

Brenda.Larcom@Zscaler.com

asparagi@hhhh.org


ZSCALER™

# Attack Resistance

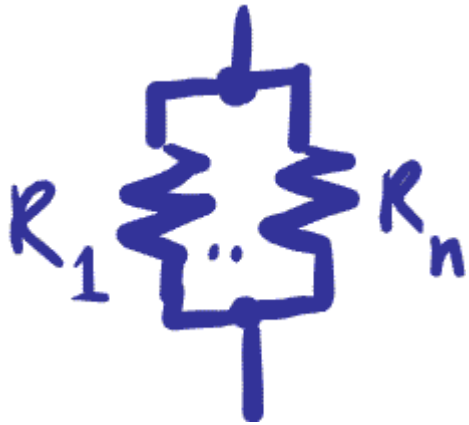



- How hard it is to get from starting privileges S to ending privileges E
- Treat functions of system components as resistors
  - Units: seconds to acquire privileges exposed by this function

# Calculating Attack Resistance


Selecting Times

- Best: as measured
  - From component library
  - Ad hoc
- Guess at design time
- For ranges, pick average or worst case consistently




In Series

- $R = R_1 + \ldots + R_n$
- More steps = harder for the attacker
- Harder possibilities make more difference

In Parallel

- $R = 1/(1/R_1 + \ldots + 1/R_n)$
- More possibilities = easier for the attacker
- Easier possibilities make more difference

# Connectivity

send + receive Ethernet traffic — IP networking stack → send + receive HTTP traffic …

## Functions/Resistors

- Every function of every component (as-designed behavior or implementation flaw)
  - Provides one or more privileges (E)
  - To users who have privileges it requires (S)
  - When the system is in a given state (C)

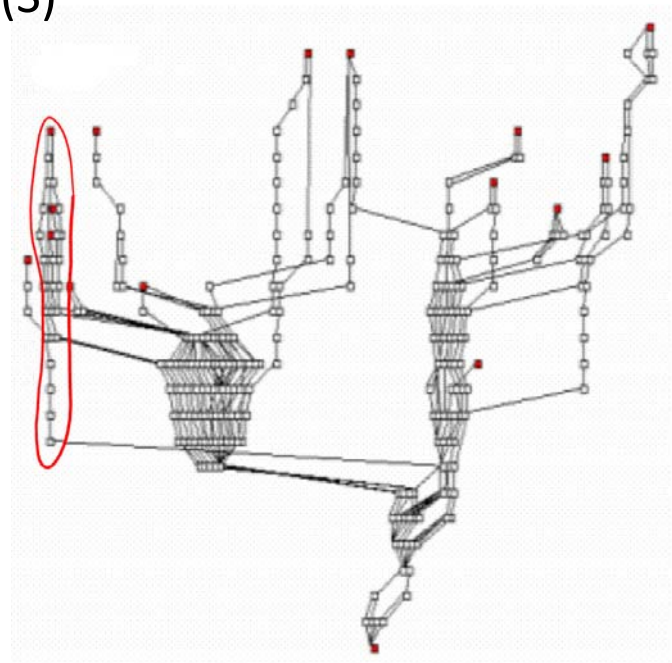
## Virtual Graph

- Conceptually, if C holds and S and accumulated E match, privileges chain

send + receive HTTP traffic → Apache → execute arbitrary code

## Generate/Prune

- Construct or select non-looping subset of graph from $S_A$ to $E_A$



ZSCALER™

# Why…

… this is useful:

- One number for prevention
  - Architecture, design, implementation or deployment
  - Different analysts
- Uses the right kinds of inputs
  - Attacker & defense goal
  - As-designed behavior
  - Known vulnerabilities
- Matches intuition about badness
- Guesses in design can be measured in implementation

… this is deeply wrong:

- These units don't act this way

… applicability is limited:

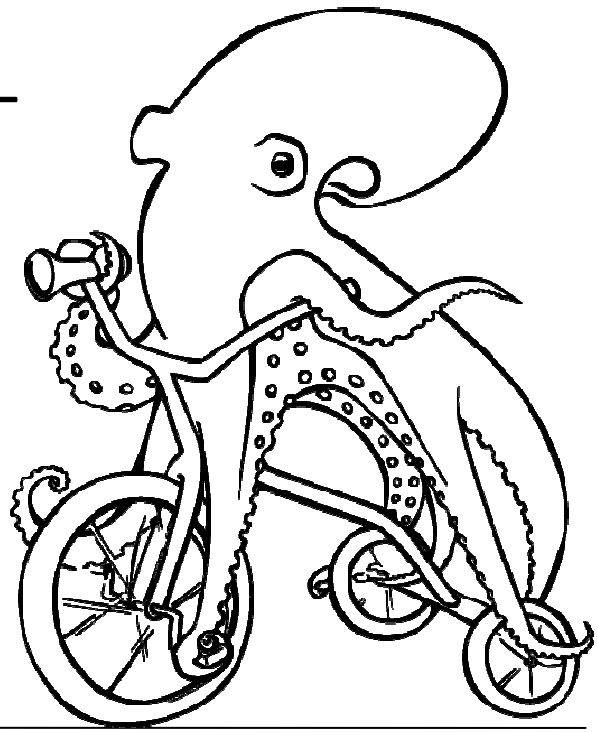
- Always worst case
- Ignores
  - Unknown vulnerabilities
  - Non-determinism
  - Non-privilege attacker characteristics

# Observations & Directions

- Attack resistance (indeed, existence) of design flaws mostly depends on environment
- Power = component's contribution to insecurity of system
  - Look at high power issues first
- Capacitance = response?
- Inductance = detection?

# Credits & References

- Steve Mancini, Ella Saitta, Erik Simmons, and Acorn Pooley helped develop this metric
- Example system from The MulVAL Project
- Network connectivity graph from CAIDA PlotPaths examples
- Tools coming in Trike v2 (http://www.octotrike.org/)



ZSCALER™