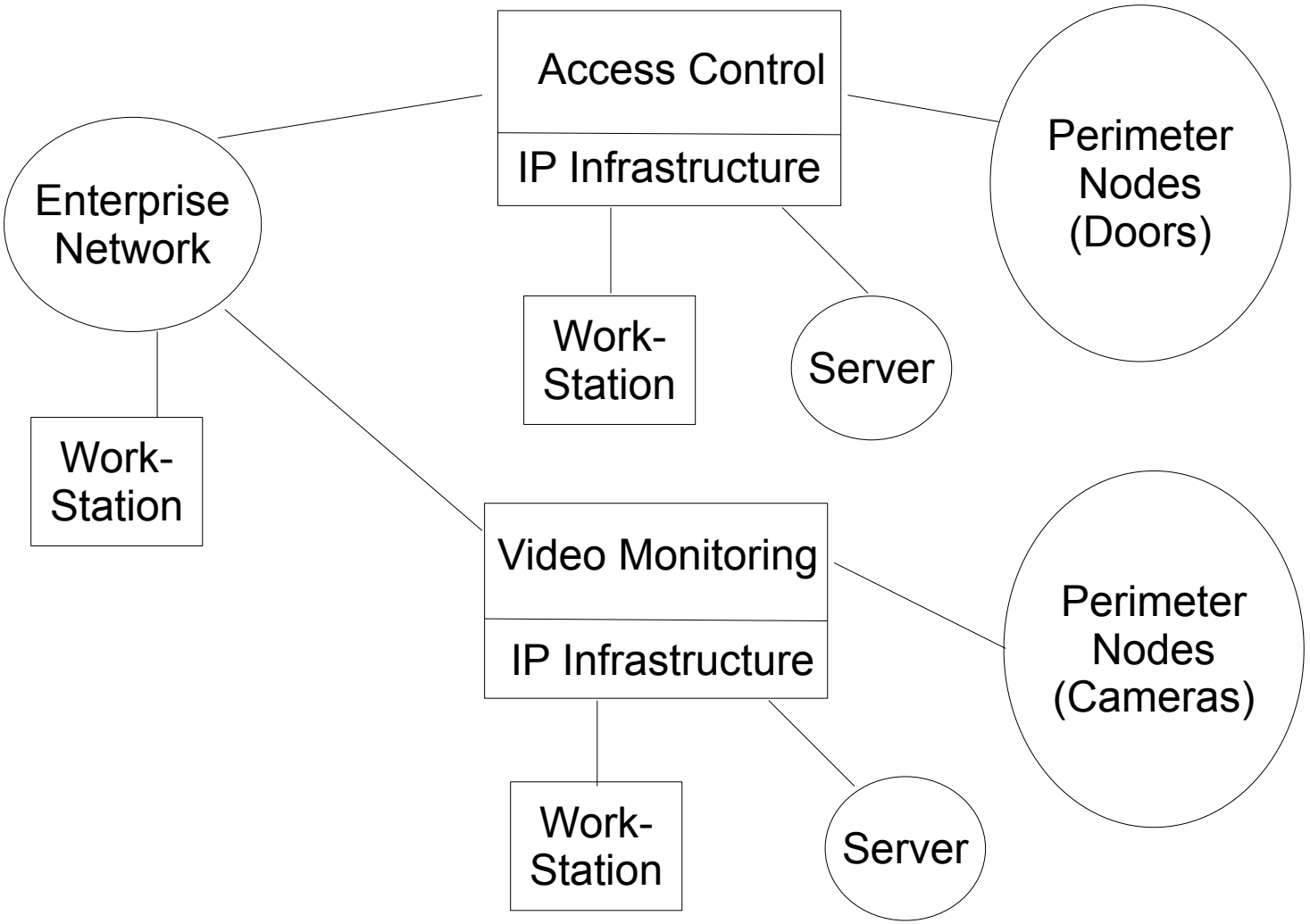
Practical Measures to Protect Your Security Systems From Insider and Outsider Attacks

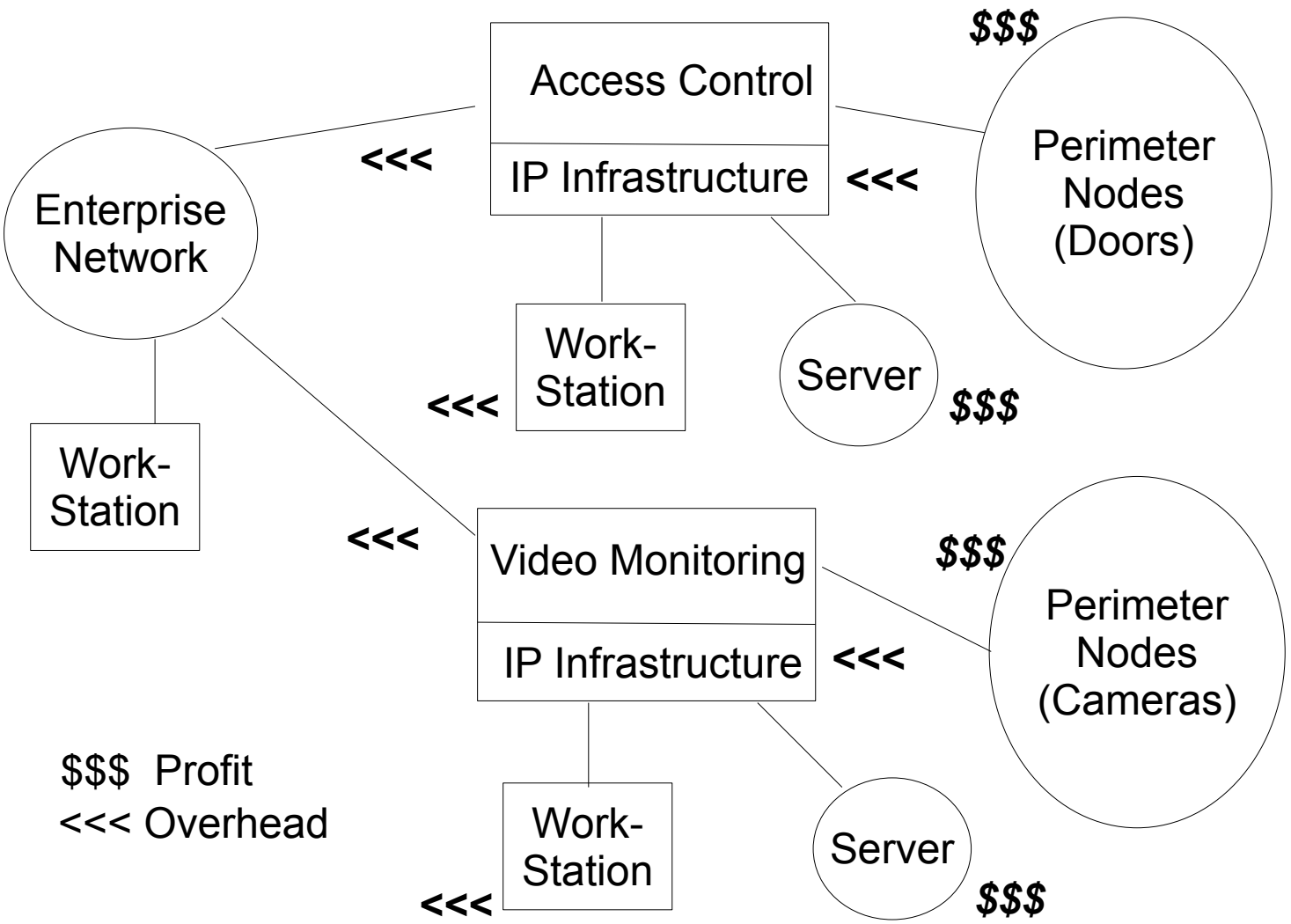
Rodney Thayer

“Shock and Awe”
What you see, what I see.

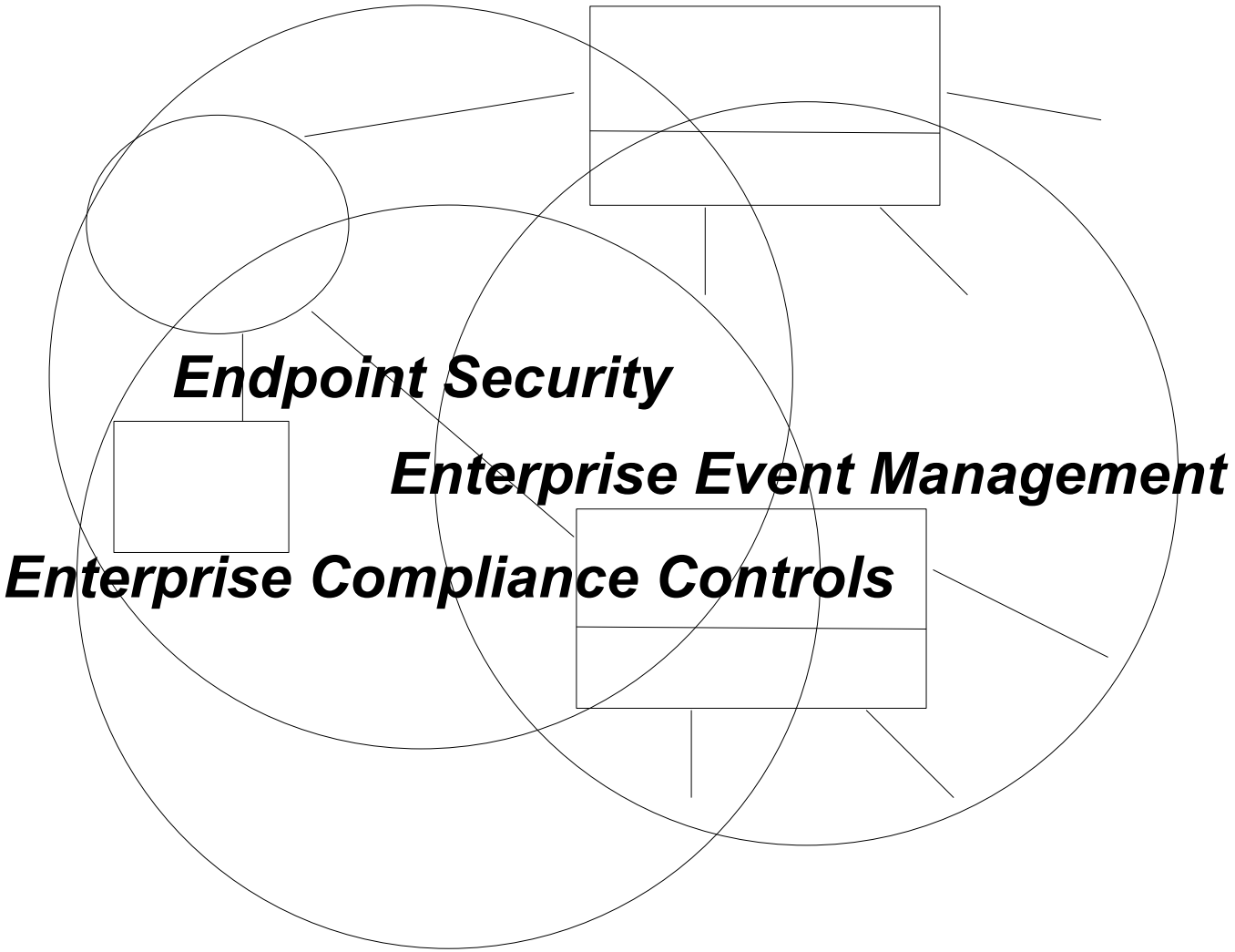
Physical Infrastructure (Practitioner's View)



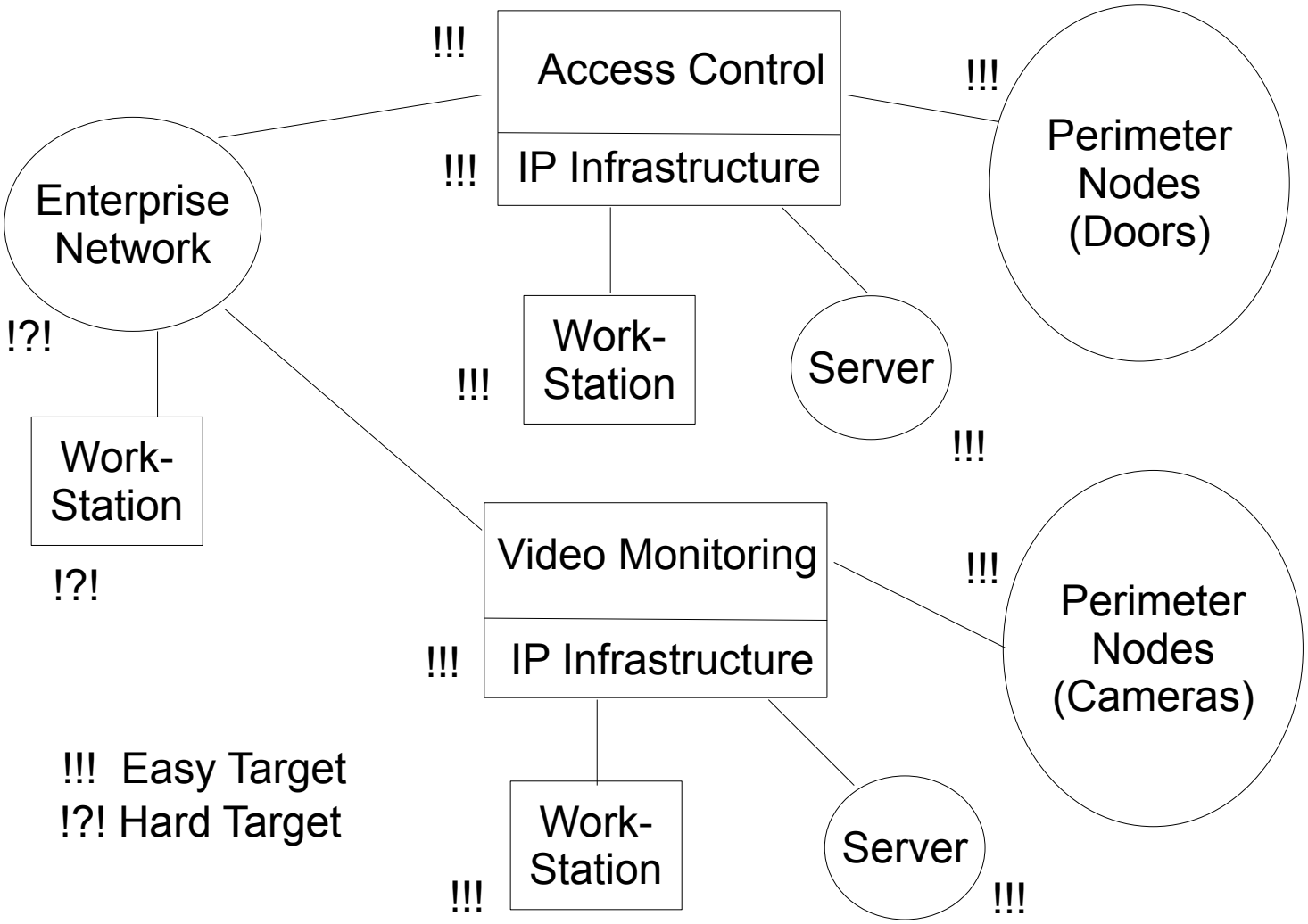
Physical Infrastructure (Vendor View)



Infrastructure (CIO View)



Physical Infrastructure (Adversary View)

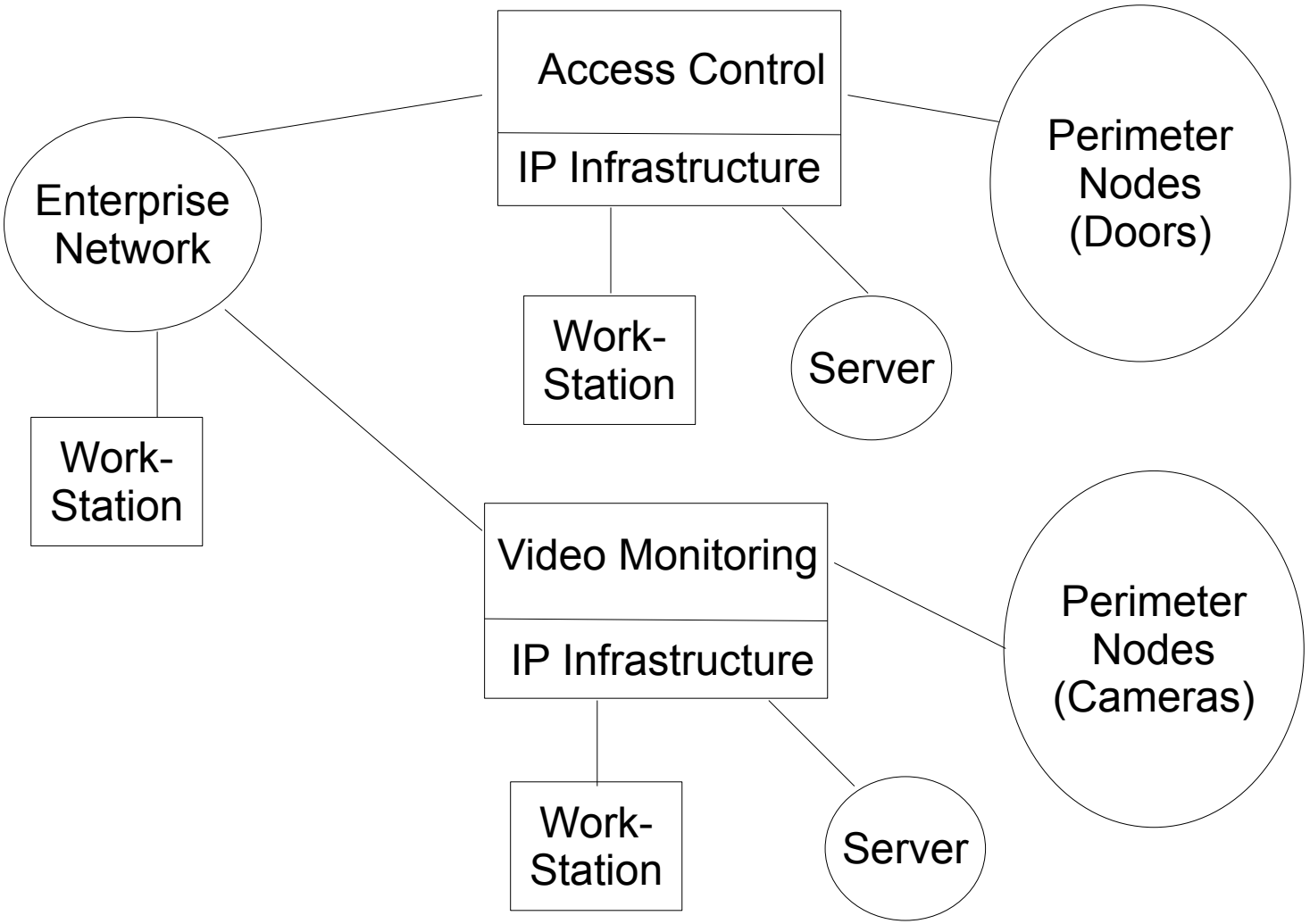


“As Built”.
(Insecurities and all)

Network Security – Practical Issues

- Everyone (no matter how big) wants to be cheap
- Use of weak networking gear
- Essentially no computer access credentials
- Little or no network hygiene (updates, a/v, backups, hardware maintenance)
- Primitive configurations

Physical Infrastructure (Practitioner's View)



Practical Measures

- Clean up your access control act
- Add minimal/primitive network management tools
- Conventional computer/network maintenance
- If necessary use conventional modern (SMB) security and network appliances

“Practical” Issues

- Network/System malware
- Performance
- Instrumentation/Telemetry
- Scalability and Maintenance

MacGuyver, Aliens, and Exotic Tools.

NOT.

Tools to secure a network

- Commercial vs. Open Source - Issues
  - Cost and Viability
  - Complexity and platform requirements
  - Practical application
- Open Source
  - (free)
  - Community maintained
  - Complexity and platform requirements

Open Source Tools

- Network tracing – TCPDUMP, Wireshark
- Network scanning – NMAP
- Linux/Posix platforms
- Hardware
  - Computer
  - Network
- Attack/Validation tools

Tools for attacking your network

- Commercial
  - Accidental
  - Malicious
- Open Source
  - Nmap
  - Traffic generators
  - Scripts

Close Encounters with Convergence

Convergence in Physical Security

- It's 2010
- Dot-com era hacking is a decade-old problem
- Decade-old network solutions are attackable
- Networks need to be stable
- Networks need to be defensible
- Networks need to be verifiable

Practical ways to deal with Convergence

- Apply 21st century network management
- Leverage open source tools
- Leverage commodity networking products
- Treat your network like a perimeter you are responsible for managing (and defending)

RSG Model Works

www.rsgmodelworks.com