Configuration Management and Security

Steven M. Bellovin
http://www.cs.columbia.edu/~smb
Columbia University

November 11, 2007

Why is Configuration Important?

- Security policy configuration for firewalls is obviously important
- What services are being run? What versions?
- What patches are installed?
- Is the desired service set contingent on the versions or patch levels?
- Has some unauthorized party changed a configuration?
- How do you manage the authorization list?
- All of this is much worse in large-scale deployment!

Security Scenarios

- Security appliances
- Infrastructure
- Servers
- Desktops and laptops

Security Appliances

- Scope: firewalls, filtering routers, etc.
- What should the configuration *be* in a complex topology?
- How do you distribute it? Verify it? Test it? Maintain and verify the topology?
- How do you reconcile different policy needs?
- In Arbor Networks' *Worldwide Infrastructure Security Report* (Sept 2007), half of respondents indicated that management of ACLs was the "most critical" missing or limited feature.
- Many corporations indicate they have similar problems

Infrastructure

- Do internal infrastructure nodes (routers, switches, etc.) have proper security configuration? (Passwords, filtering, logging, addresses, etc.)
- How do you know if some element's configuration is wrong?
- How do you know if it's been changed?
- How do you configure new nodes in the far reaches of your net?

Servers

- What services are running?
- What versions of those services?
- Again: how do you monitor changes, new nodes, etc.?

Personal Machines

- As before: what services, versions, changes, etc.?
- How do you balance personal needs and preferences with corporate policy?
- How do you enforce — or prevent — upgrades?
- How do you change the configuration of laptop or home computers?
- How do you balance central control and policy with the very varied environments laptops experience?

Summary

- Specifying the desired configuration is hard
- Distributing and monitoring it is hard
- Reconciling conflicting configurations is hard
- But it's on the front line of security