Tim Boerner

April 25, 2013

CS598 Network Security

Operational Network Security

or how I learned that the purpose of network security has little to do with actually securing the network

Introduction

Thinking about Security

Evaluating Security Requirements

Conclusion

Introduction

- Where this lecture is coming from (my background)
- Where this lecture is going (my goal)
- Speak up or I’m going home

Definition

Operational Network Security

taking the concepts from the fields of network and systems security and implementing them to address real-world problems under the constraints of real-world situations

understanding the security threats present for a given network environment and being able to determine sufficient countermeasures for these threats

Context

- As a Network Operator
- As a Network Security Researcher
- The range of network environments is vast

Introduction

Thinking about Security

Evaluating Security Requirements

Conclusion

A Philosophical Dichotomy

- The network should be completely open. You should design your network to facilitate packet flow. If you need security, then that's a host problem.
- The network is a battlefield. You must design your network such that traffic routes through choke points for monitoring and access control. Allow no reconnaissance of your network or its resources. Host-based security is your last line of defense.

- Since I mentioned the whole "open network" thing …

Network Security as an Expression of Organizational Culture

- Network security efforts reflect the mindset of the organization
- Trusting work environment vs. untrusting work environment
- Restrictions on computer use could impact employee attitude
- Crafting policies leads to expectations of employee behavior

Network Security as a Policy Framework

- The network security agenda is typically set by the executives
- A set of policies defined by an organization to guide use of the network
  - Acceptable use policies
  - Data access policies
- Informs network design and security measures taken
- Policy can provide a framework assign blame

Questioning Network Security

- Is more network security always a good thing?
- In what ways does increased network security negatively impact other design features of a given network that are generally considered to be important or valuable to an organization?

- How much network security is enough?
- How much network security is enough to protect an organization's valued data, services, and the productivity of its employees from the majority of security threats that it is likely to experience given threats present on the network today?

Network Security Trade-Offs

Security vs. …

- Usability
- Performance
- Flexibility
- Cost

Security vs. Usability

- The most easily used networks have no barriers to productivity
- The most secure networks are powered off
- Examples of security technologies that impact usability:
  - Microsoft's User Account Control (UAC)
  - Network Access Control (NAC)
  - Password complexity requirements
- Can security measures be so onerous that they negatively impact employee job satisfaction?

Security vs. Performance

- The fastest networks place no restrictions on access to, or transfer of, data
- The most secure networks evaluate the security impact of every byte as it is read or before it is transferred
- Examples of security technologies that impact performance:
  - Stateful Packet Inspection (SPI)
  - Antivirus Software
- Are there any situations where it is unacceptable to have any active security devices between a host and the Internet?

Security vs. Flexibility

- The most flexible networks have no constraints on their design
- The most secure networks are restricted in how they can be designed or extended
- Examples of security policies that impact flexibility:
  - Security audits for connectivity to partner networks
  - Security zoning between datacenters

Security vs. Cost

- The most least expensive networks spend money only on functionality
- The most secure networks spend more on security than on functionality
- Examples of security technologies that are expensive:
  - High speed `$SECURITY_DEVICE`
  - System-wide event correlation
  - Vendor lock-in
- Note: What an organization sees as expensive is usually relative to its size.

Introduction

Thinking about Security

Evaluating Security Requirements

Conclusion

Two Easy Steps

- It’s simple to secure your network, just follow these two easy steps:
  - design a secure network
  - implement that design
- Wait! What?

What are we securing?

- Physical Devices
  - Servers, desktops, laptops, routers, switches
- Services
  - Web sites, databases, phone systems, email
- Resources
  - Network connectivity, company data

Why should we secure it?

- Data
  - Intellectual property
  - Personal data (privacy)
  - National security
  - Legal regulations
- Services
  - Customer-facing products (e.g. eCommerce sites, “the cloud”)
  - Reputation
- Resources
  - Employee productivity
  - Value from investment

A Closer Look at Why: Data

- To determine how much data security is warranted, we must understand the value of the data itself
- Two ways to assess the value data
  - Expense of losing access to data
  - Expense of others gaining access to data
- Examples:
  - Amateur photographer vs. professional photographer
  - Oil and gas company

A Closer Look at Why: Productivity

- Nonproductive employees impact the “bottom line”
  - Idle employees don’t earn money
  - Idle employees still get paid

- Examples to consider:
  - Employees spend too much time on facebook and youtube

    [1,000 Employees] x [1 Hour / Day] x [$30 / Hour] =
    $30,000 Lost Every Day

  - The offline law firm

    [100 Attorneys] x [4 Hours] x [$300 / Hour] =
    $120,000 Lost Revenue

A Closer Look at Why: Legal Regulations

- Laws and regulations have been passed that require certain data to be secured
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Sarbanes-Oxley Act of 2002 (SOX or SARBOX)
  - Gramm-Leach-Bliley Act (GLBA)
  - Payment Card Industry (PCI) Data Security Standard
- Non-compliance typically comes with fines
- Rather than examples, some questions to ponder:
  - Why did these laws need to be created in the first place?
  - If the fine for non-compliance is less costly than becoming compliant, is that company likely to become compliant?

Pause to Consider

What are the trends we're seeing so far?

There are two main reasons that we secure our network and data assets, money and principles.

How should we secure it?

- Baseline security measures against pervasive threats (e.g. firewall, antivirus)
- Some security measures are taken spontaneously*
  - (when they have measureable benefits, are easy to manage, and inexpensive)
- Security beyond the minimum
  - Understand the threat
  - Cost to secure vs. risk of loss
  - Impact to usability, performance, flexibility

- "… the blinking thing is our security?"

A Closer Look at How: Mostly Secure

- General, external threats are more straight-forward to address
- You can get mostly secure with a few generic security measures
  - Strong password policies
  - Firewall external connections
  - Managed antivirus on all systems
  - Email filtering (anti-spam, anti-phishing, etc)
  - Web filtering (ad blocking, malicious site blocking, etc)
- Internal threats can be tricky to deal with
- Advanced persistent threats (APTs) aren’t fun either

A Closer Look at How: Measuring Risk

- This is something that executives do behind closed doors
- Some general steps to gauge what is sufficient security
  - List threats to a given resource
  - Assign probabilities to these threats' ability to compromise the resource
  - Assign costs associated with the resource being compromised
  - How much can you reduce the likelihood of a compromise without exceeding the value of the resource?
- Additional considerations when considering security measures
  - Impact to usability, performance, flexibility

Pause to Consider

Good network security doesn't just prevent your system from being compromised, it also grants you insight into what happened *after* your system has been compromised or misused.

Who did what on your system and how do you prove it?

What can you afford to not know about what is happening on your network?

How do you correlate all of the data that you might receive from the thousands of systems reporting back to you?

Introduction

Thinking about Security

Evaluating Security Requirements

Conclusion

Closing Thoughts

- How network security is implemented can be interpreted as an expression of organizational culture
- In the corporate world, network security is about mitigating risk
- Sometimes, though, security is about principles
- There are no one size fits all solutions out there
- Wait! Where's the hardware?