

# Secure Networks

Starting with  
Basic Reference Model for Security Architecture

A Historic Review of a Nascent Industry

Seattle University – CSSE 572 – Spring 2008

Mohsen Banan – Guest Speaker

May 15, 2008

# Less Talked About Security Topics

Network is the Computer

Network is the Software

Network is the Service

Secure the Network

We are not going to go far without a

Reference Model

Plenty to be learned from past mistakes and successes

X.509: The basis of most of today's security

Security of Internet Mail: A Case Study

More Philosophy

The Future

# Class Readings

- Why Those Two Documents?
  - 1) 7498-2 -- X.800
  - 2) X.509

# Importance Of Reference Models Security Architecture and Vocabulary

History of 7498-2 (X.800)

Why so neglected and unused?

First generation Internet humans:

How are we to establish vocabulary for new  
concepts?

What a mess without it.

Internet is not always neat. Stuff happens.

Talk Properly.

Robustness Principle:

Be conservative about what you say and liberal about  
what you hear.

# Importance of X.509

- Father/Seed of much of today's security facilities.
- Historic Significance
- Why in the X.500 series? – The Directory
- Why after 20 years still not widespread?
- PKCS
- PKI and Certificate Infrastructure

# The Directory

A Quick Tour

# Cryptography

- Symmetric Cryptography – Secret Key
  - DES
- Asymmetric Cryptography – Public Key – PKCS
  - RSA
- Combination of the two

# PKCS – PKI –

## Why it has not been hapening?

- Centralized Infrastructures take a long time in the capitalistic models.
- PGP – Organic efforts fill some gaps.
- Patent fights don't help. (RSA patents)
- Real engineers should eventually prevail.

# Security of Internet Email

## A Case Study

- History
  - 1986 Snap Shot
  - 1990 Snap Shot
  - 1994 Snap Shot
  - 2006 Snap Shot

# Simple vs Good vs Complex

- Early in the evolution of the Network, Simple kills Complex everytime.
  - RFC-822+SMTP vs X.400
- Early in the evolution of the Network, Simple kills Good everytime.
  - In order to be good it had to be more complex
- Later in the evolution of the Network, you have to get it right and be good.

# Symptoms Management Vs Cure

## A Culture Of Patches

- Architecture and Protocols
  - Vs
- Patches and Software
- Meaningful Evolutionary Steps

# Misc. Less Talked About Security Topics

- Lessons Learned
- Choices of Approach and Philosophy

# Security By Obscurity

VS

# Security Through Transparency

- Abandoned VMS boxes hardly ever get hacked
- If you are running Debian GNU/Linux put getting of security updates in cron.
- Stay with the mainstream and update often.
- Generally, I like my hardware fresh and software well done.
- But, even well done software needs to be refreshed to remain secure.

# Diversity in the Gene Pool Makes Things More Secure

- In our Data Center we run:
  - X86 - Debian Sarge GNU/Linux
  - Sparc – Debian Sarge GNU/Linux
  - Sparc Solaris

# Hide Your Topology

- NATs are not always evil.
- Redirection also has security benefits.

# Recover Quick

- What to do after you have been compromised?
- We target the ability of reconstructing any box based on an updated OS in a matter of minutes.
  - Easier said than done!

# Why Were We Attacked?

- People with less enemies get attacked less often.
- The ultimate security is total vulnerability, where the only thing between you and the next guy is his conscience.
  - Too crazy?

# Network Security Landscape in 2008

- $2008 - 20 = 1988$
- $2008 + 20 = 2028$
- Security will always remain a tradeoff analysis.

# Questions and Discussions

- ???