Network Security

A Quick Overview

Joshua Hill

josh-web@untruth.org

http://www.untruth.org

Security Engineering

- What is “Security Engineering”?
  - "Security Engineering is about building systems to remain dependable in the face of malice, error or mischance." -- Ross Anderson

Goals

- What are the goals of security engineering?
  - Depends on system
  - Traditionally things like: confidentiality, data integrity, entity authentication, message authentication, signatures, authorization, validation, access control, certification, timestamping, witnessing, receipt, confirmation, ownership, anonymity, non-repudiation, revocation, assurance...

Assurance: What you say?

- Security
  - Actual resistance to attack
    - What sort of attack?
    - What sort of attacker?
  - Complex to quantify (intangible)
- Assurance
  - Degree of belief that “Security” level is correct.
  - Also intangible

Snake Oil, Inc.

- Ridiculous claims
  - “One Time Pad!”
  - “1,000,000 bit keys!”
  - “Completely Unbreakable!”
  - “Revolutionary!”
  - “Inverse N-dimensional permutation matrix routed through the exhaust manifold and the main deflector dish, with a twist of lemon.”
- No assurance at all.
  - Secret/Unevaluated/Under-evaluated systems

Assurance for Dummies

- (Competent) Peer Review
- Standards Compliance
  - Common Criteria
  - FIPS PUBS
    - FIPS 140-2, FIPS 180-2, FIPS 186-2...
- “Good Practice”
- Independent Evaluation

OK... So Now What?

- How can the general system security goals be satisfied in reasonable (verifiable/quantifiable) ways, particularly in distributed settings?
  - Generally a Hard Problem ™
  - Good understanding of the problem and security engineering is important

Security Engineering Patterns

- Simplicity
- Complete Mediation
- Separation of Privilege
- Least Privilege
- Least Common Mechanism
- Defense in Depth
- Open Design
- Auditability
- Physiological Acceptability

Auditability

- Policy
  - CONOPS
  - Security Policy
    - Corporate
    - Network
  - Design Documentation
- Procedure
  - Administration

Network Security Policy

- What are the Security Domains?
  - What are the rules for each domain?
    - What connections are allowed?
    - What sort of information exchange is permitted?
  - How can security domains interact?

NSP Application

- How can it be applied?
  - Architecturally
    - Network Design should make domains natural
    - Device/Host configuration should be consistent with NSP
  - Enforcement of the NSP
    - Firewalls
  - Verification of the NSP
    - IDSes
- Where?
  - Most critical at Security Domain Boundaries

Network Design

- Ethernet Hubs
  - 1 Collision Domain / 1 Broadcast Domain
  - No security benefit
- Ethernet Switches (Normal)
  - Multiple Collision Domains / 1 Broadcast Domain
  - Limited security benefit
- Ethernet Switches (VLAN)
  - Multiple Collision / Broadcast Domains
  - Limited security benefit
- Routers
  - Multiple Collision / Broadcast Domains
  - Multiple independent segments
  - Reasonable security segmentation

Firewalls

- Stateless (basic packet filter)
  - Complex rulesets
  - Simplest design
  - Least granularity
- Stateful
  - Basic
    - Understands some underlying protocols
    - More symbolic (generally simpler) rulesets
    - Moderate Complexity
  - Proxy
    - Most control over traffic
    - Most complex
    - Understands all protocols in use

IDSes

- Host based
  - Analysis of host logging information
- Network based
  - Network monitoring (sniffing)
  - “Interactions” with switches

Common Failures

- Switches as security devices
- Incorrectly placed firewalls
- Misplaced trust in IDSes
- Logging trauma
- Lack of understanding of underlying protocols

Trust Management

- System design in terms of trust
- Extending trust
  - Policy/Procedures
  - Laws/Regulation
  - Technical Solutions

Technical Measures

- Cryptography can help
- Has primitives to help establish
  - Confidentiality
  - Data integrity
  - Authentication
  - Non-repudiation

Cryptographic Primitives

- Random number generation
- Stream ciphers
- Block ciphers
- Public key encryption
- Cryptographic hash functions
- MACs
- Public key signatures

Trust Extension

- Each primitive has a set of attributes
- Primitives are used in a Security Protocol
- Security Protocol can be used to extend trust in various ways

SSL/TLS

- Client has:
  - CA public certificate
  - Possibly client certificate
- Server has:
  - Server certificate
- Trust relationships
  - Client and Server trust CA
  - Client Trusts Real Server
  - Server may trust Client
- Trust is extended through
  - RNGs, Hashes, PK Signatures, PK encryption, Block (or stream) ciphers, MACs

IPSec/IKE

- Endpoints have
  - Authentication data (various sorts)
- Trust relationships
  - Endpoints trust each other
  - Endpoints trust authentication data (and associated infrastructure)
- Trust is extended through
  - RNGs, Hashes, MACs, Block Ciphers
  - “Other Stuff” for IKE

There and Back Again

A Packet's Tale

- VPNs attempt to emulate trusted connections
  - Can encapsulate complete packets
  - Can provide confidentiality, data authentication
  - Virtual "trusted piece of wire"

Crypto-Modules

- Offer crypto-in-a-box
- Can be more secure than “integrated crypto”
  - Smaller
  - More fully evaluated
  - Can be leveraged to make big, complex systems more secure

Quantifying Security

- What sort of attackers?
  - How well funded are they?
  - What resources do they have access to?
  - How risk adverse are they?
  - How much time do they have?
  - Where in the system do they start?
  - What expertise/information do they have?

Attacker Modeling

- Computationally unbounded (IT model)
- Computationally bounded
- Monetarily / Time bounded

General Analysis

- Risk Analysis
- Attack Trees

Summary

- Security is Hard
  - It is intangible
  - It is complex
  - Its goals are difficult to define
- Assurance is often ignored
- There are several Techniques to help
- Network security is even more hard and complex