

Network Security - ISA 656 Review

Angelos Stavrou

December 3, 2008



- The Exam
- The Exam
- Material**
- Test Conditions
- Introduction
- Web & Email Security
- IPsec
- Applications (SSH & VoIP)
- Intrusion Detection
- Worms and Denial of Service

Material

- If it's in my slides or I said it in class, you're responsible for it
- There may be some questions based on the Labs
- You're responsible for the assigned Labs and Homeworks at about the level of class coverage.



- The Exam
- The Exam**
- Material
- Test Conditions
- Introduction
- Web & Email Security
- IPsec
- Applications (SSH & VoIP)
- Intrusion Detection
- Worms and Denial of Service

The Exam

- 7:20pm - 10:0pm, Tuesday, Dec 10th, in the Lab (STI-128)
- Same style of questions as the midterm
- I'm not asking you to write programs



- The Exam
- The Exam
- Material
- Test Conditions**
- Introduction
- Web & Email Security
- IPsec
- Applications (SSH & VoIP)
- Intrusion Detection
- Worms and Denial of Service

Test Conditions

- Open book
- Open notes, posted code, manuals, Labs...
- You can bring a calculator but save your energy; you won't need it
- No laptops, IM, Chatting, or phones...

Terminology

- The Exam
- Introduction
- Terminology**
- Kinds of Threats
- Assets
- Web & Email Security
- IPsec
- Applications (SSH & VoIP)
- Intrusion Detection
- Worms and Denial of Service

- Confidentiality, integrity, availability
- Threats, attacks, and vulnerabilities

Assets

- The Exam
- Introduction
- Terminology
- Kinds of Threats
- Assets**
- Web & Email Security
- IPsec
- Applications (SSH & VoIP)
- Intrusion Detection
- Worms and Denial of Service

- Protect what?
- Bandwidth, CPU, data, identity
- Attacker powers?

Kinds of Threats

- The Exam
- Introduction
- Terminology
- Kinds of Threats**
- Assets
- Web & Email Security
- IPsec
- Applications (SSH & VoIP)
- Intrusion Detection
- Worms and Denial of Service

- Joy hackers
- Criminals
- Competitors
- Nation states
- Insiders

SSL

- The Exam
- Introduction
- Web & Email Security
- SSL**
- Web Certificates
- Browser Security
- Continuing Authentication
- Web Server Security
- Email Security
- Phishing
- Defenses
- IPsec
- Applications (SSH & VoIP)
- Intrusion Detection
- Worms and Denial of Service

- What is SSL?
- Client authentication types
- Properties and requirements
- Uses
- Trust model

Web Certificates

- [The Exam](#)
- [Introduction](#)
- [Web & Email Security](#)
- [SSL](#)
- [Web Certificates](#)**
- [Browser Security](#)
- [Continuing Authentication](#)
- [Web Server Security](#)
- [Email Security](#)
- [Phishing](#)
- [Defenses](#)
- [IPsec](#)
- [Applications \(SSH & VoIP\)](#)
- [Intrusion Detection](#)
- [Worms and Denial of Service](#)

- Root certificates
- The browser vendor's role
- Bindings
- Human factors

Continuing Authentication

- [The Exam](#)
- [Introduction](#)
- [Web & Email Security](#)
- [SSL](#)
- [Web Certificates](#)
- [Browser Security](#)
- [Continuing Authentication](#)**
- [Web Server Security](#)
- [Email Security](#)
- [Phishing](#)
- [Defenses](#)
- [IPsec](#)
- [Applications \(SSH & VoIP\)](#)
- [Intrusion Detection](#)
- [Worms and Denial of Service](#)

- Cookies
- Embedded values
- Cryptographically sealing data

Browser Security

- [The Exam](#)
- [Introduction](#)
- [Web & Email Security](#)
- [SSL](#)
- [Web Certificates](#)
- [Browser Security](#)**
- [Continuing Authentication](#)
- [Web Server Security](#)
- [Email Security](#)
- [Phishing](#)
- [Defenses](#)
- [IPsec](#)
- [Applications \(SSH & VoIP\)](#)
- [Intrusion Detection](#)
- [Worms and Denial of Service](#)

- Why is it a problem?
- Active content
- Javascript
- ActiveX

Web Server Security

- [The Exam](#)
- [Introduction](#)
- [Web & Email Security](#)
- [SSL](#)
- [Web Certificates](#)
- [Browser Security](#)
- [Continuing Authentication](#)
- [Web Server Security](#)**
- [Email Security](#)
- [Phishing](#)
- [Defenses](#)
- [IPsec](#)
- [Applications \(SSH & VoIP\)](#)
- [Intrusion Detection](#)
- [Worms and Denial of Service](#)

- Why?
- Trust model
- Scripts and their dangers
- Injection attacks
- Permissions

Email Security

- [The Exam](#)
- [Introduction](#)
- [Web & Email Security](#)
- [SSL](#)
- [Web Certificates](#)
- [Browser Security](#)
- [Continuing Authentication](#)
- [Web Server Security](#)
- [Email Security](#)
- [Phishing](#)
- [Defenses](#)
- [IPsec](#)
- [Applications \(SSH & VoIP\)](#)
- [Intrusion Detection](#)
- [Worms and Denial of Service](#)

- Usual evaluation
- How to sign and encrypt?
- Details
- Threats: eavesdropping, password theft, spool file

Defenses

- [The Exam](#)
- [Introduction](#)
- [Web & Email Security](#)
- [SSL](#)
- [Web Certificates](#)
- [Browser Security](#)
- [Continuing Authentication](#)
- [Web Server Security](#)
- [Email Security](#)
- [Phishing](#)
- [Defenses](#)
- [IPsec](#)
- [Applications \(SSH & VoIP\)](#)
- [Intrusion Detection](#)
- [Worms and Denial of Service](#)

- Mutual authentication
- Personalization
- DKIM
- Non-reusable credentials
- (MITM attacks; human factors)

Phishing

- [The Exam](#)
- [Introduction](#)
- [Web & Email Security](#)
- [SSL](#)
- [Web Certificates](#)
- [Browser Security](#)
- [Continuing Authentication](#)
- [Web Server Security](#)
- [Email Security](#)
- [Phishing](#)
- [Defenses](#)
- [IPsec](#)
- [Applications \(SSH & VoIP\)](#)
- [Intrusion Detection](#)
- [Worms and Denial of Service](#)

- What is it?
- How it's done
- Tracing

IPsec

- [The Exam](#)
- [Introduction](#)
- [Web & Email Security](#)
- [IPsec](#)
- [IPsec](#)
- [Attacking IPsec](#)
- [Applications \(SSH & VoIP\)](#)
- [Intrusion Detection](#)
- [Worms and Denial of Service](#)

- What is IPsec, and why?
- ESP and AH
- SPI
- SAs
- Tunnel and transport mode
- VPN and their use model

Attacking IPsec

- [The Exam](#)
- [Introduction](#)
- [Web & Email Security](#)
- [IPsec](#)
- [Attacking IPsec](#)**
- [Applications \(SSH & VoIP\)](#)
- [Intrusion Detection](#)
- [Worms and Denial of Service](#)

- Cut-and-paste attacks
- Probable plaintext
- Interactions with other layers

SSH

- [The Exam](#)
- [Introduction](#)
- [Web & Email Security](#)
- [IPsec](#)
- [Applications \(SSH & VoIP\)](#)
- [SSH](#)**
- [SIP](#)
- [Intrusion Detection](#)
- [Worms and Denial of Service](#)

- Features
- Security model
- Client authentication
- Connection-forwarding
- SSH Agent

Applications

- [The Exam](#)
- [Introduction](#)
- [Web & Email Security](#)
- [IPsec](#)
- [Applications \(SSH & VoIP\)](#)
- [Applications](#)**
- [SSH](#)
- [SIP](#)
- [Intrusion Detection](#)
- [Worms and Denial of Service](#)

- SSH
- SIP

SIP

- [The Exam](#)
- [Introduction](#)
- [Web & Email Security](#)
- [IPsec](#)
- [Applications \(SSH & VoIP\)](#)
- [Applications](#)
- [SSH](#)
- [SIP](#)**
- [Intrusion Detection](#)
- [Worms and Denial of Service](#)

- SIP architecture
- What's at risk?
- Protecting voice versus signaling
- What type of crypto is used where
- Complex scenarios

What is IDS?

- The Exam
- Introduction
- Web & Email Security
- IPsec
- Applications (SSH & VoIP)
- Intrusion Detection
- What is IDS?**
- Limits of Network IDS
- IDS Architecture
- Worms and Denial of Service

- Purpose
- Host versus network IDS
- Logs and traces

IDS Architecture

- The Exam
- Introduction
- Web & Email Security
- IPsec
- Applications (SSH & VoIP)
- Intrusion Detection
- What is IDS?
- Limits of Network IDS
- IDS Architecture**
- Worms and Denial of Service

- Detector
- Database
- Analyzer
- Countermeasures
- Signature versus Anomaly-based sensors
- Polymorphism and IDS Limitations

Limits of Network IDS

- The Exam
- Introduction
- Web & Email Security
- IPsec
- Applications (SSH & VoIP)
- Intrusion Detection
- What is IDS?
- Limits of Network IDS**
- IDS Architecture
- Worms and Denial of Service

- Insertion and evasion attack
- Checksum errors
- TTLs
- TCP normalization

Worms

- The Exam
- Introduction
- Web & Email Security
- IPsec
- Applications (SSH & VoIP)
- Intrusion Detection
- Worms and Denial of Service
- Worms**
- Denial of Service
- Routing Attacks
- Wireless Security

- Worms versus viruses
- Spread: program versus social engineering
- Payloads
- Spam
- Detection

Denial of Service

- The Exam
- Introduction
- Web & Email Security
- IPsec
- Applications (SSH & VoIP)
- Intrusion Detection
- Worms and Denial of Service
- Worms
- Denial of Service**
- Routing Attacks
- Wireless Security

- Types of DOS attack
- TCP attacks
- DDoS
- Defenses & Limitations

Wireless Security

- The Exam
- Introduction
- Web & Email Security
- IPsec
- Applications (SSH & VoIP)
- Intrusion Detection
- Worms and Denial of Service
- Worms
- Denial of Service
- Routing Attacks
- Wireless Security**

- Evil twin
- Battery lifetime
- WEP — why the crypto is bad
- War-driving
- Access control

Routing Attacks

- The Exam
- Introduction
- Web & Email Security
- IPsec
- Applications (SSH & VoIP)
- Intrusion Detection
- Worms and Denial of Service
- Worms
- Denial of Service
- Routing Attacks**
- Wireless Security

- Why they happen
- Goals
- Defenses and their effectiveness