

Network Security - ISA 656 Review

Angelos Stavrou

December 4, 2007



- The Exam
- The Exam
- Material**
- Test Conditions
- Introduction
- Cryptography
- Web Security
- IPsec
- Applications
- 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
- Cryptography
- Web Security
- IPsec
- Applications
- Intrusion Detection
- Worms and Denial of Service

The Exam

- 7:20pm - 9:30pm, Thursday, Dec 11th, 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
- Cryptography
- Web Security
- IPsec
- Applications
- 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](#)
- [Cryptography](#)
- [Web Security](#)
- [IPsec](#)
- [Applications](#)
- [Intrusion Detection](#)
- [Worms and Denial of Service](#)

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

Kinds of Threats

- [The Exam](#)
- [Introduction](#)
- [Terminology](#)
- [Kinds of Threats](#)
- [Assets](#)
- [Cryptography](#)
- [Web Security](#)
- [IPsec](#)
- [Applications](#)
- [Intrusion Detection](#)
- [Worms and Denial of Service](#)

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

Assets

- [The Exam](#)
- [Introduction](#)
- [Terminology](#)
- [Kinds of Threats](#)
- [Assets](#)
- [Cryptography](#)
- [Web Security](#)
- [IPsec](#)
- [Applications](#)
- [Intrusion Detection](#)
- [Worms and Denial of Service](#)

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

Ciphers

- [The Exam](#)
- [Introduction](#)
- [Cryptography](#)
- [Ciphers](#)
- [Public Key Cryptography](#)
- [Certificates](#)
- [Web Security](#)
- [IPsec](#)
- [Applications](#)
- [Intrusion Detection](#)
- [Worms and Denial of Service](#)

- What is a cryptosystem?
- What is a block cipher? What are generic properties of block ciphers?
- What are the different modes of operation? What are their properties? When would you use each mode?
- What is a stream cipher?

Public Key Cryptography

- The Exam
- Introduction
- Cryptography
- Ciphers
- Public Key Cryptography**
- Certificates
- Web Security
- IPsec
- Applications
- Intrusion Detection
- Worms and Denial of Service

- What is it? What is it good for? Limitations?
- How are public key systems used?
- Random numbers and where they come from
- Digital signatures

Certificates

- The Exam
- Introduction
- Cryptography
- Ciphers
- Public Key Cryptography
- Certificates**
- Web Security
- IPsec
- Applications
- Intrusion Detection
- Worms and Denial of Service

- Trust properties
- CAs
- Authorization versus identity certificates
- Web of trust
- Types of certificates
- Revocation

SSL

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

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

Web Certificates

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

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

Browser Security

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

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

Continuing Authentication

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

- Cookies
- Embedded values
- Cryptographically sealing data

Web Server Security

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

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

Email Security

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

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

Phishing

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

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

Defenses

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

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

IPsec

- [The Exam](#)
- [Introduction](#)
- [Cryptography](#)
- [Web Security](#)
- [IPsec](#)
- [IPsec](#)**
- [Packet Processing](#)
- [Attacking IPsec](#)
- [Applications](#)
- [Intrusion Detection](#)
- [Worms and Denial of Service](#)

- What is IPsec, and why?
- ESP and AH
- SPI
- SAs
- Tunnel and transport mode

Packet Processing

- [The Exam](#)
- [Introduction](#)
- [Cryptography](#)
- [Web Security](#)
- [IPsec](#)
- [IPsec](#)
- [Packet Processing](#)**
- [Attacking IPsec](#)
- [Applications](#)
- [Intrusion Detection](#)
- [Worms and Denial of Service](#)

- Outbound and inbound
- SPD and SADB
- Rule characteristics

Attacking IPsec

- [The Exam](#)
- [Introduction](#)
- [Cryptography](#)
- [Web Security](#)
- [IPsec](#)
- [IPsec](#)
- [Packet Processing](#)
- [Attacking IPsec](#)
- [Applications](#)
- [Intrusion Detection](#)
- [Worms and Denial of Service](#)

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

Applications

- [The Exam](#)
- [Introduction](#)
- [Cryptography](#)
- [Web Security](#)
- [IPsec](#)
- [Applications](#)
- [Applications](#)
- [SSH](#)
- [SIP](#)
- [Intrusion Detection](#)
- [Worms and Denial of Service](#)

- SSH
- SIP
- Networked storage

SSH

- [The Exam](#)
- [Introduction](#)
- [Cryptography](#)
- [Web Security](#)
- [IPsec](#)
- [Applications](#)
- [Applications](#)
- [SSH](#)
- [SIP](#)
- [Intrusion Detection](#)
- [Worms and Denial of Service](#)

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

SIP

- [The Exam](#)
- [Introduction](#)
- [Cryptography](#)
- [Web Security](#)
- [IPsec](#)
- [Applications](#)
- [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](#)
- [Cryptography](#)
- [Web Security](#)
- [IPsec](#)
- [Applications](#)
- [Intrusion Detection](#)
- [What is IDS?](#)
- [Limits of Network IDS](#)
- [IDS Architecture](#)
- [Worms and Denial of Service](#)

- Purpose
- Host versus network IDS
- Logs and traces

Limits of Network IDS

- [The Exam](#)
- [Introduction](#)
- [Cryptography](#)
- [Web Security](#)
- [IPsec](#)
- [Applications](#)
- [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

IDS Architecture

- [The Exam](#)
- [Introduction](#)
- [Cryptography](#)
- [Web Security](#)
- [IPsec](#)
- [Applications](#)
- [Intrusion Detection](#)
- [What is IDS?](#)
- [Limits of Network IDS](#)
- [IDS Architecture](#)
- [Worms and Denial of Service](#)

- Detector
- Database
- Analyzer
- Countermeasure
- Signature versus anomaly

Worms

- [The Exam](#)
- [Introduction](#)
- [Cryptography](#)
- [Web Security](#)
- [IPsec](#)
- [Applications](#)
- [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](#)
- [Cryptography](#)
- [Web Security](#)
- [IPsec](#)
- [Applications](#)
- [Intrusion Detection](#)
- [Worms and Denial of Service](#)
- [Worms](#)
- [Denial of Service](#)**
- [Routing Attacks](#)
- [Wireless Security](#)

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

Routing Attacks

- [The Exam](#)
- [Introduction](#)
- [Cryptography](#)
- [Web Security](#)
- [IPsec](#)
- [Applications](#)
- [Intrusion Detection](#)
- [Worms and Denial of Service](#)
- [Worms](#)
- [Denial of Service](#)
- [Routing Attacks](#)**
- [Wireless Security](#)

- Why they happen
- Goals
- SBGP, SO-BGP

Wireless Security

- [The Exam](#)
- [Introduction](#)
- [Cryptography](#)
- [Web Security](#)
- [IPsec](#)
- [Applications](#)
- [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