The NSA's Role In Computer Security

Adrien Cheval
Joe Willage

Introduction

- NSA was created in 1952
- Located in Ft. Meade, Maryland
- Cryptographic intelligence agency of the U.S. government
  - Part of the Department of Defense
- Approximately 30,000 employees
- Has other facilities, such as the Texas Cryptology Center, in San Antonio
- If the NSA was a corporation, in terms of dollars spent, floor space, and personnel, it would be in Fortune 500's top 10%

NSA Headquarters, MD

Introduction (cont)

- Responsible for protecting the government's information systems
    - As of January 2008, NSA is the lead agency to monitor the government's computer networks
    - Involves lots of cryptography!
- Mainly focus on foreign communication
    - But they also have a little domestic involvement
- Includes eavesdropping in many forms
    - Phone calls
    - Internet
    - Any other intercepted form of communication

Introduction (cont)

- The NSA has not only played a large role in our government
  - They have developed many of the cryptographic protocols used in a large amount of systems today

- **DES**
- Clipper Chip
- **AES**
- SKIPJACK cipher
- Fortezza
- Duel EC DRBG pseudorandom number generator
- **SELinux**
- Type 1 Encryption
- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

SHA Hashes!

Data Encryption Standard (DES)

- A need for encrypting sensitive data was identified by the Federal Government in 1972
- NSA put out a solicitation for proposals
- IBM took them up on the offer
  - Introduced a Block Cipher with a 64 bit block size
  - Key size to be 56 bits with 8 bits for parity
  - Consists of 16 rounds of the same method
  - Encryption completely reversible as long as key is known, due to the properties of XOR

DES Adopted as a Standard

- DES was approved as a federal standard in 1976
- Reaffirmed as a standard in 1983, 1988, and 1993
- As time progressed, computers got more powerful

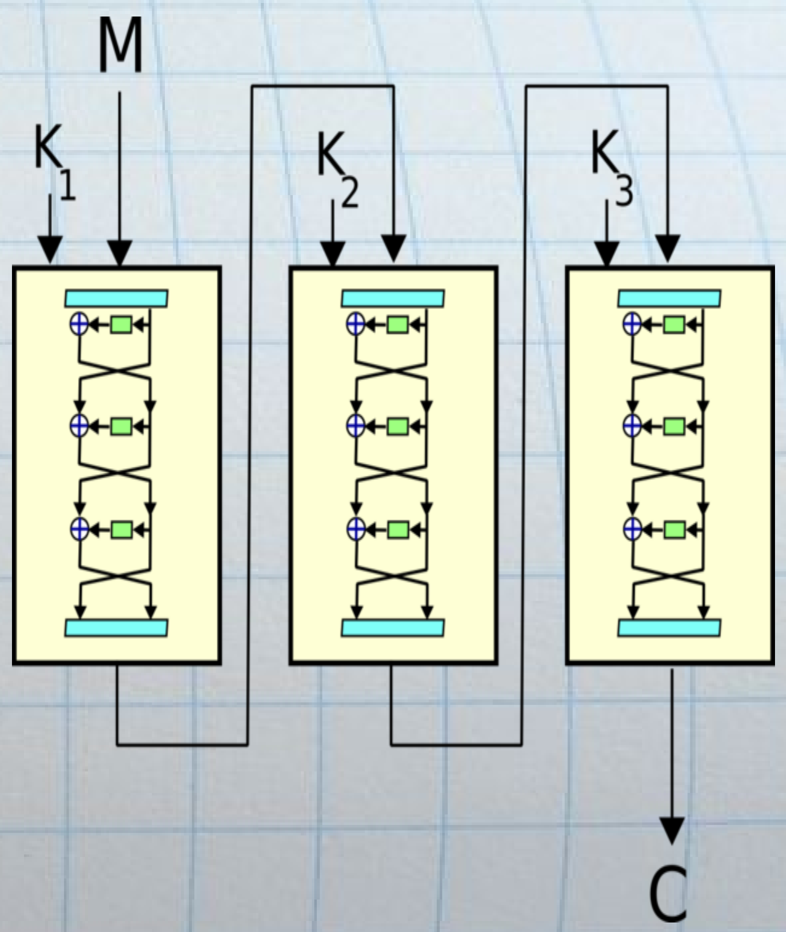
- Moore's Law
  - A transistor will decrease in size by a factor of 2 every 18 months
- DES became susceptible to attacks in the 1990's

- In 1998, the EFF built a custom DES-cracker for $250,000

Triple DES (TDES)

- Replace DES in 1999 as a federal standard
- Involves 2 keys, each 56 bits long
- Ciphertext = Ek1(Dk2(Ek1 (Plaintext)))

- Three iterations of DES (48 total rounds)
- Approved by the National Institute of Standards and Technology (NIST) for sensitive information until 2030



New Encryption Standard Introduced

- Although TDES was approved for sensitive information until 2030, many felt there was a better solution
  - TDES suffers from slow performance on modern processors
  - It is better suited to hardware implementations
    - VPN Appliances
    - NEXTEL Cellular and Data Network
  - Unfortunately, data requiring encryption is often stored in bits and software, not to mention websites on the internet

Advanced Encryption Standard (AES)

- NIST declared in 1997 that it wanted
  - an unclassified, publicly disclosed algorithm
  - capable of protecting sensitive government information
  - well into the next century

- NIST announced that AES became effective as a Federal Standard in 2002

- Created by two Belgian Cryptographers, Joan Daemen and Vincent Rijmen

- As of 2006, it is the most popular algorithm used in Public Key Cryptography

Why AES is the New Standard

AES is amazing because ...

- 6 times faster than TDES
- Very simple to implement in both hardware and software
- Requires very little memory
- Due to these properties, it is being deployed on a large scale

AES is Unique

- Available by choice in many encryption packages
- First time that the public has access to a cipher approved by the NSA for TOP SECRET information

Properties of AES

Cipher Key Detail

- Key size can be 128 bits, 192 bits, or 256 bits (variable key length)

Number of Rounds

- 128 bit key - 10 rounds
- 192 bit key - 12 rounds
- 256 bit key - 14 rounds

Block Details

- Must be 128 bits
- Fixed length
- 128 bits / 8 = 16 bytes
- Represented in a 4x4 array of bytes
- Each block is processed in an identical fashion

AES Rounds

Four AES Operations performed during AES Rounds

1. SubBytes Operation
2. Shift Rows Operation
3. Mix Columns Operation
4. AddRoundKey Operation
5.

These rounds will be explained in more detail

Round Details

1. Initial Round
   - only AddRoundKey Operation performed
2. Final Round
   1. SubBytes Operation
   2. ShiftRows Operation
   3. AddRoundKey Operation

All other rounds employ all 4 Operations

Initial Round- AddRoundKey Operation

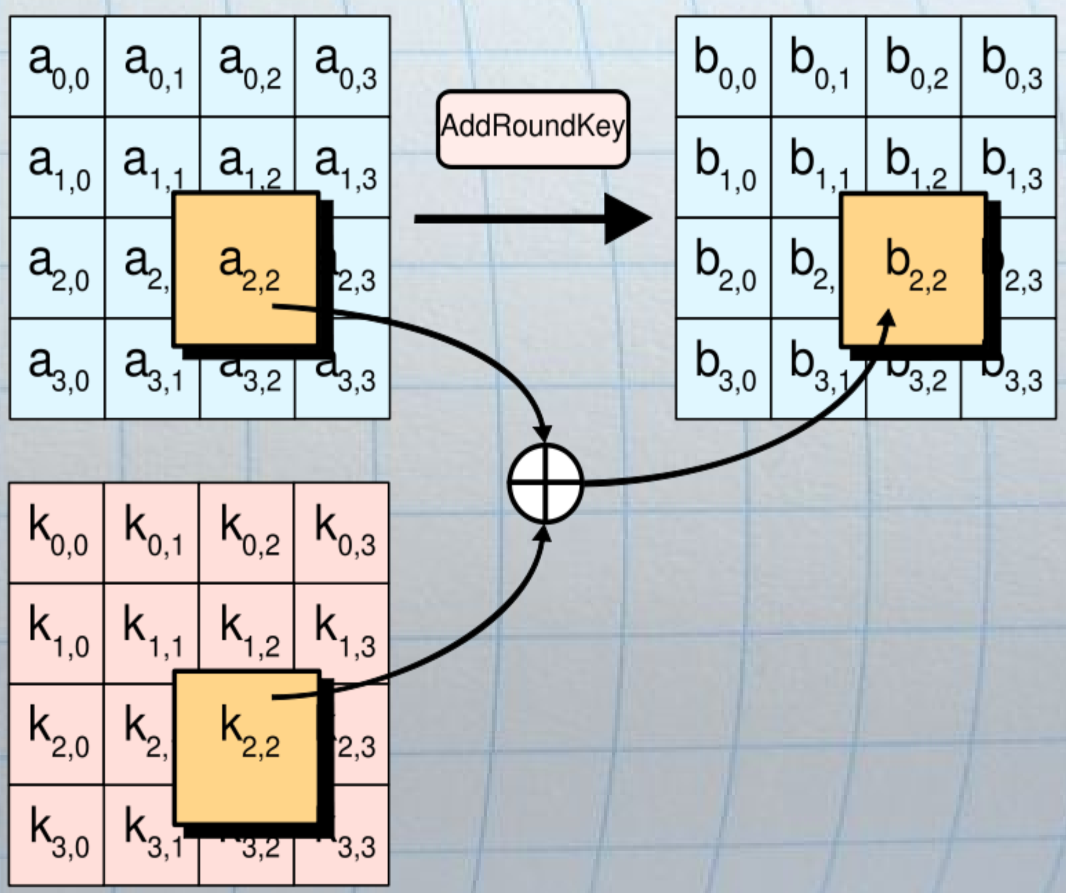
Ingredients

- 128 bit/16 byte block stored in 4x4 byte array(a), 128 bit subkey (k) which is obtained through [Rijndael's key schedule only if the key is larger than 128 bits (192 or 256 bits)]

Method

- Each byte in the block is xored with the corresponding byte in the key block
- The result of the xor is stored in the 4x4 byte array (b)

AddRoundKey Illustrated



AES - Middle Rounds

- All rounds between the first and last rounds have the same operations in AES

- Each round between the first and last Round consists of the following:
  1. Sub Bytes Operation
  2. Shift Rows Operation
  3. Mix Columns Operation
  4. AddRoundKey Operation, which was just demonstrated on the previous slide

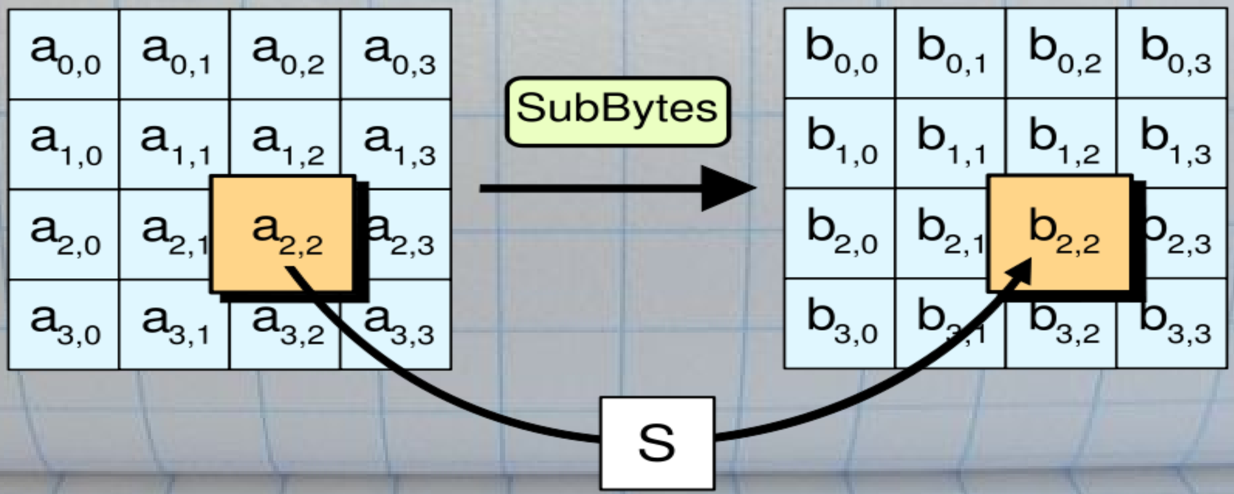
AES Middle Round- Step 1: SubBytes Operation

Ingredients

- 128 bit/16 byte/4x4 byte array (a)
- 8 bit substitution box (S-Box), which is known to have good non-linear properties
- Ideal for avoiding attacks based on simple algebraic properties

Method

1. Each byte a(i,j) is substituted into the S-Box a(i,j) = SBox[a(i,j)] and the result a(i,j) is stored in its corresponding b(i,j) entry
2. Note: The S-Box is completely independent of any input



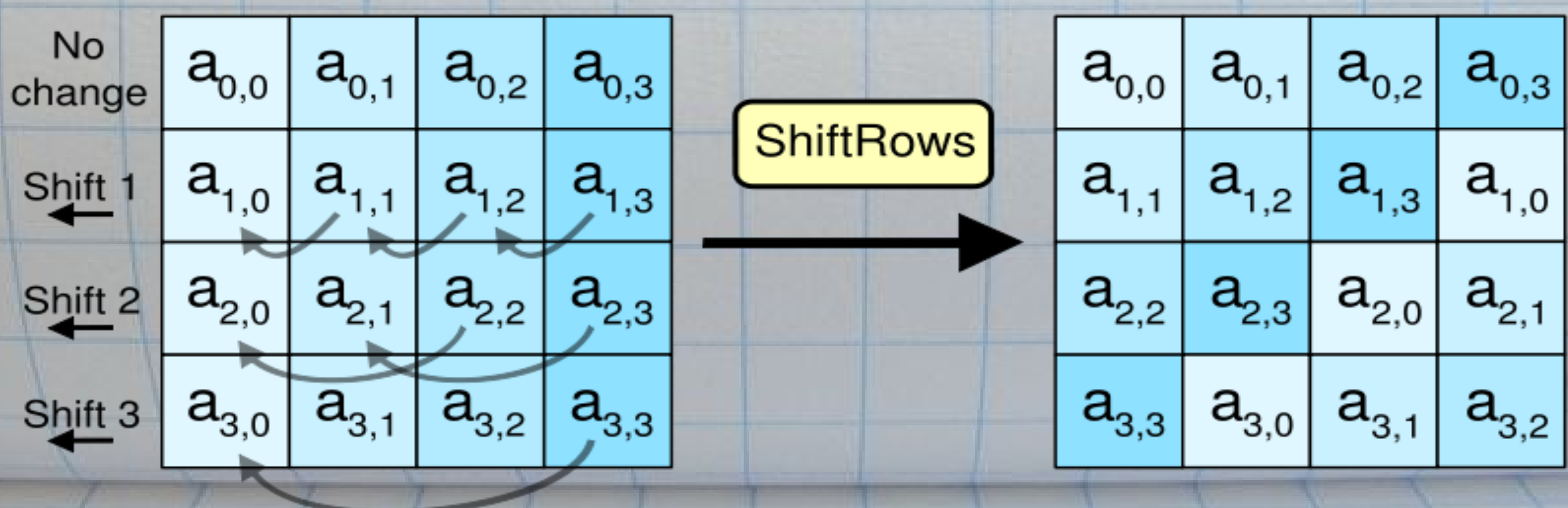
AES Middle Round Step 2: Shift Rows Operation

General Information

- Operates on the rows, and NOT the columns
- Bytes are always shifted to the left
- The amount shifted to the left is entirely dependent on the row number

Method

1. The 1st row is shifted 0 positions to the left
2. The 2nd row is shifted 1 positions to the left
3. The 3rd row is shifted 2 positions to the left
4. The 4th row is shifted 3 positions to the left



AES Middle Round Step 3: Mix Column Operation

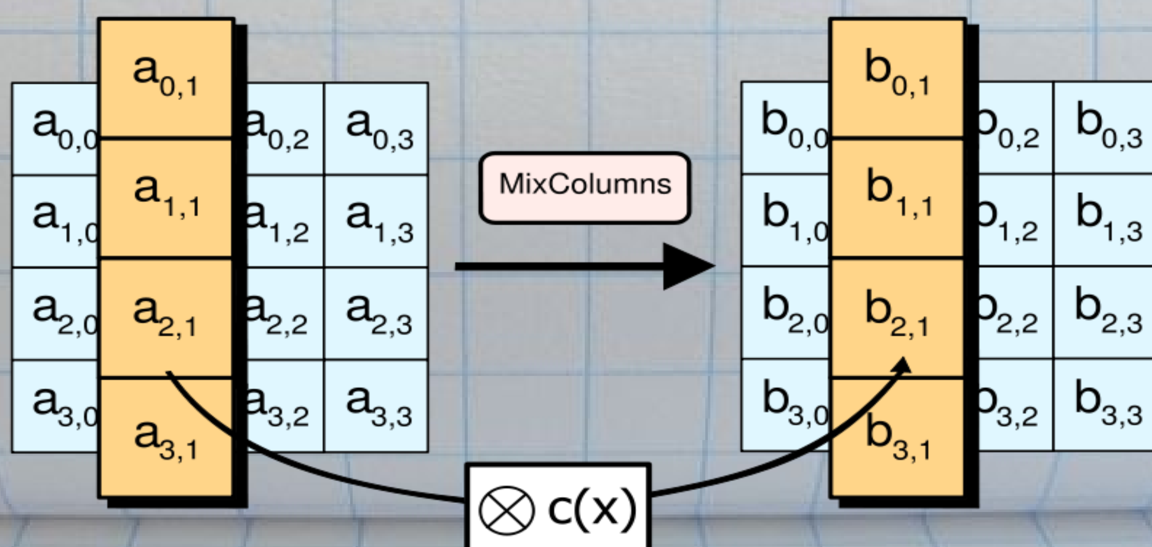
Method

- Involves advanced mathematical calculations in [Rijndael's finite field]
- Four bytes of each column of the state are combined using an invertible [linear transformation]
- Takes four bytes as input and outputs four bytes
- When combined with shift rows, provides diffusion in the cipher

- Diffusion refers to the property that redundancy in the statistics of the plaintext is removed in the statistics of the ciphertext
- This is very powerful, it ensures that statistical properties cannot be used to break the encryption

Steps

1. Each column treated as a polynomial and multiplied modulo $x^4 + 1$ with a fixed polynomial $c(x) = 3x^3 + x^2 + x + 2$



AES Middle Round Step 4: AddRoundKey

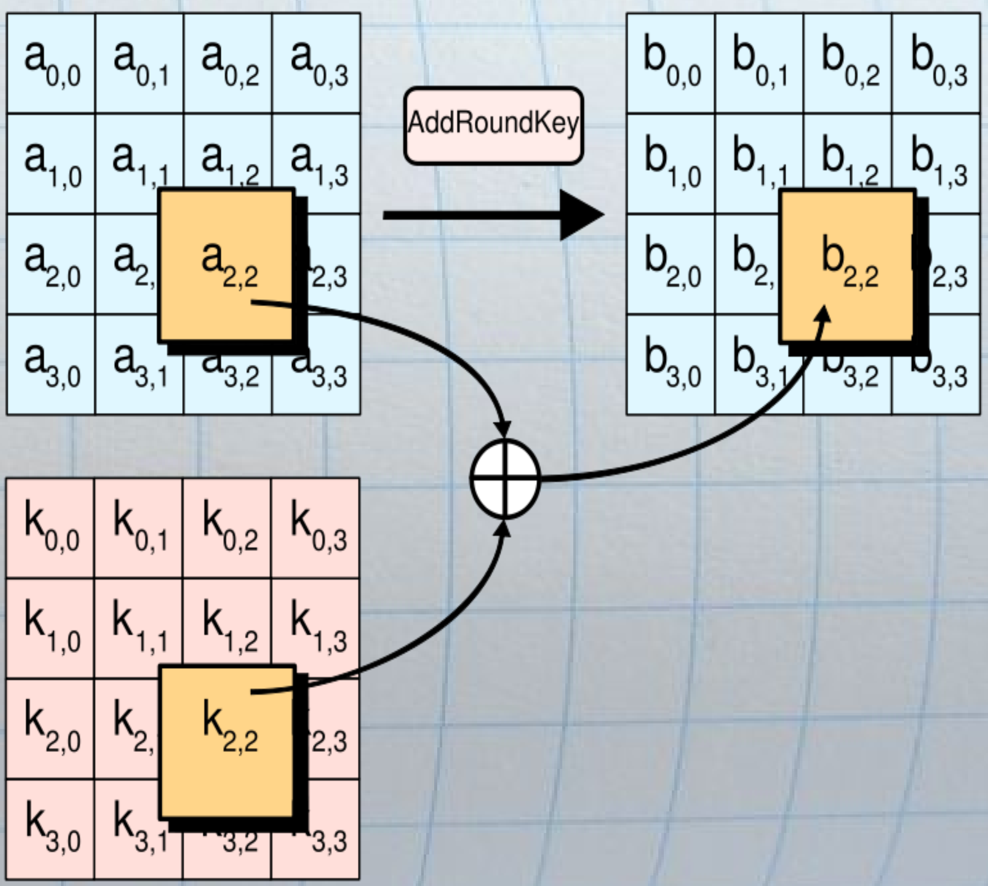
Ingredients

- 128 bit/16 byte block stored in 4x4 byte array(a), 128 bit subkey (k) which is obtained through [Rijndael's key schedule only if the key is larger than 128 bits (192 or 256 bits)]
- If the key is 128 bits we can use the original key and not the subkey

Method

- Each byte in the block is xored with the corresponding byte in the key block
- The result of the xor is stored in the 4x4 byte array (b)

AddRoundKey Illustrated



AES Final Round

- The Final round is the 10th, 12, or 14th round, depending on whether the key is 128 bits, 192 bits, or 256 bits, respectively

- The Final Round involves all of the operations except for MixColumn
    1. SubBytes
    2. ShiftRows
    3. AddRoundKey

- In order to obtain the plaintext from the ciphertext, one must have the key

Attacks on AES

- Side Channel Attacks are not very practical
- There are more traditional approaches attempts at breaking AES
  - Related Key Attack
    - Can Break up to 9 rounds of 256-bit key AES
    - Falls short of the 14 rounds of AES for 256 bits
  - Chosen Plaintext Attack
    - Can Break up to 8 rounds of 192-bit and 256-bit key
    - Still falls short of the 12 rounds for 192 bits
    - Can Break up to 7 rounds of 128 bit, which is the closest one (by three rounds)

- In conclusion: the weakest form of AES is 128 bits

SHA hash functions

- Includes 5 algorithms
  - SHA-1
  - SHA-224
  - SHA-256
  - SHA-384
  - SHA-512
- Typically just referred to as SHA-1 and SHA-2
- The naming is easy!
  - SHA stands for Secure Hash Algorithm
  - SHA-1 produces a 160 bit digest
  - The numbers in the SHA-2 functions denote the length of the digest

SHA hash funcions (cont)

- SHA-1
  - Published in 1995
  - Based on MD4 message digest algorithm
  - Revision of the original function (SHA-0)
  - Differed only by 1 bitwise rotation, but proven to be stronger
  - Undergone much more scrutiny, and has much wider use than SHA-2 (~2001)

SHA hash functions (cont)

SHA-1 example:

SHA-1(Mike Burmester is the greatest professor)
= b25479b3baf58852fb8dfb24ac116c6a57d9af18

SHA-1(Mike Burmester is th**f** greatest professor)
= ec988dc6cec0436aabcaa1de1ced3ff3fa3025d7

40 hex characters * 4 bits per character = 160 bit digest

SHA hash functions (cont)

- How secure is SHA?
  - Can be broken in an average of 2^L/2 evaluations, where L is the bit length of the SHA output
  - For SHA-1 (160 bit digest), this means 2^80 evaluations
  - "80-bit strength"
- SHA-1 is so popular, that a collision search is being made using BOINC in Graz University of Technology in Austria

SHA applications

- SHA-1 is the most widely used version
- Many applications
  - SSL
  - TSL
  - IPsec
  - PGP
  - SSH
  - S/MIME
  - DSS
- Required by law for some US government applications
- P2P filesharing
  - Identify files
  - Verify content

Misc SHA information

- Before SHA-1, what's now called SHA-0 existed briefly, from 1993 until SHA-1 in 1995
- SHA-3
  - An open competition to develop the new hash function
  - Announced Nov 2007, ran through Oct 2008
  - The winner and new publication will be announced in 2012!

SELinux

- Security Enhanced Linux!
- Not a distro
  - Modifications that can be installed in any Unix OS
- Provides security policies and mandatory access controls
- Can enforce the policy over all objects and processes
- OPEN SOURCE
- Released in 2000
  - Integrated in version 2.6 in 2003

SELinux (cont)

- Quote from NSA SELinux team:
  - "It provides a mechanism to enforce the separation of information based on confidentiality and integrity requirements, which allows threats of tampering and bypassing of application security mechanisms to be addressed and enables the confinement of damage that can be caused by malicious or flawed applications."

SELinux (cont)

- SELinux inforces MAC polifies
  - Users only have the minimum privileges required to do their job
    - Reduces the chance that one of these programs can cause harm if compromised
- No idea of root user
  - Doesn't have short comings of other Linux security devices that depend on setuid/gid bits
  - Programs can still have bad configurations, but will not effect the rest of the system

SELinux (cont)

- SELinux available with commercial support in Red Hat version 4+
  - Targeted to aim at maximum ease of use
- Also supported by
  - Debian
  - Ubuntu
  - Fedora
  - Gentoo
  - Yellow Dog Linux

Sources

- All of the pictures and the diagrams were taken from sources which are cited in our paper