CIS 551 / TCOM 401

Computer and Network Security

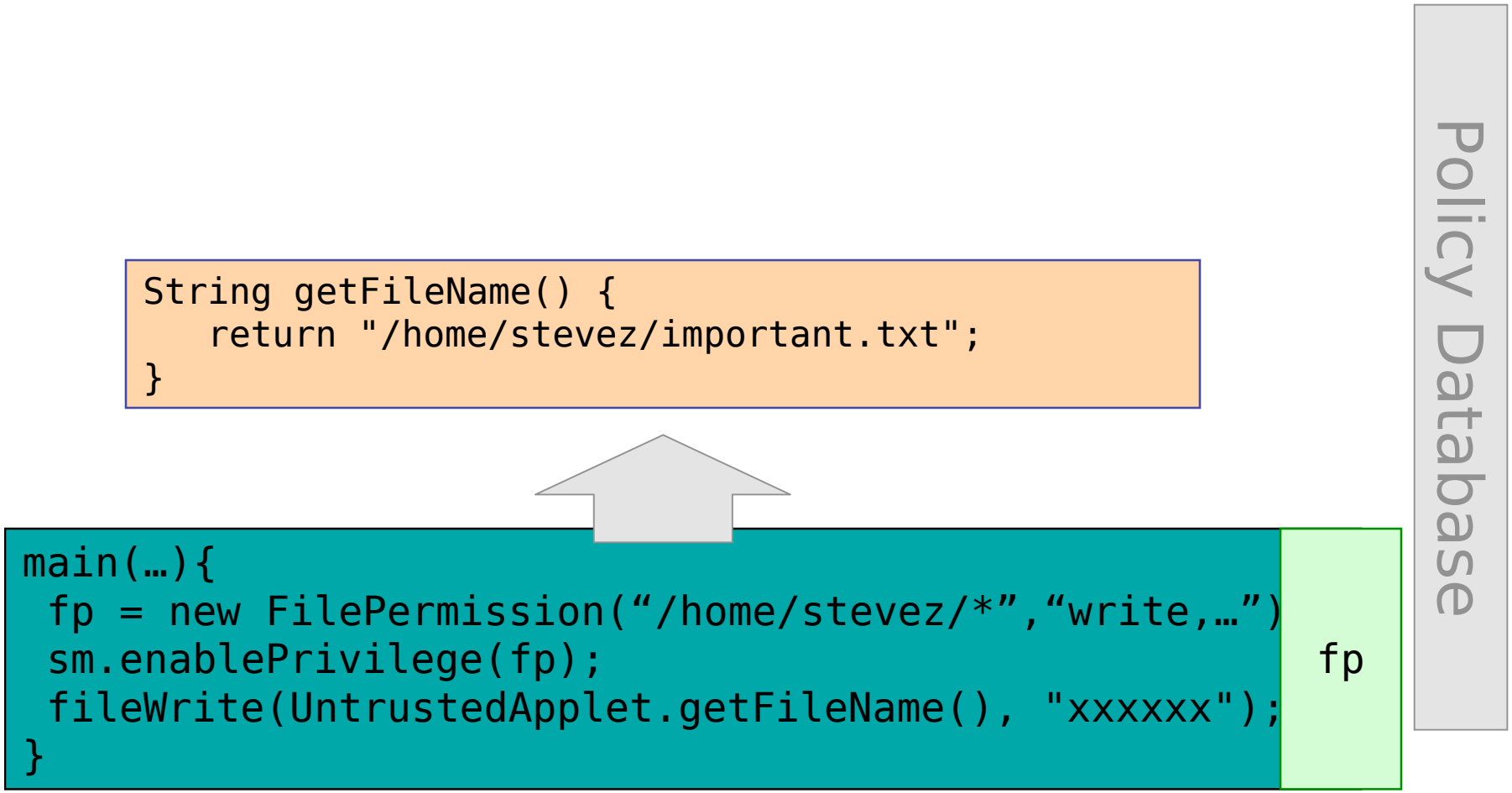
Spring 2008
Lecture 8

Announcements

- Project 1 has been graded.
- Project 2: will be posted this week
  - Due March 7th
  - Network intrusion detection
- Midterm I will be held in class next week
  - February 19th
  - Covers all material in class so far
  - Example exams from past instances are on the web (note: material was covered in a different order…)

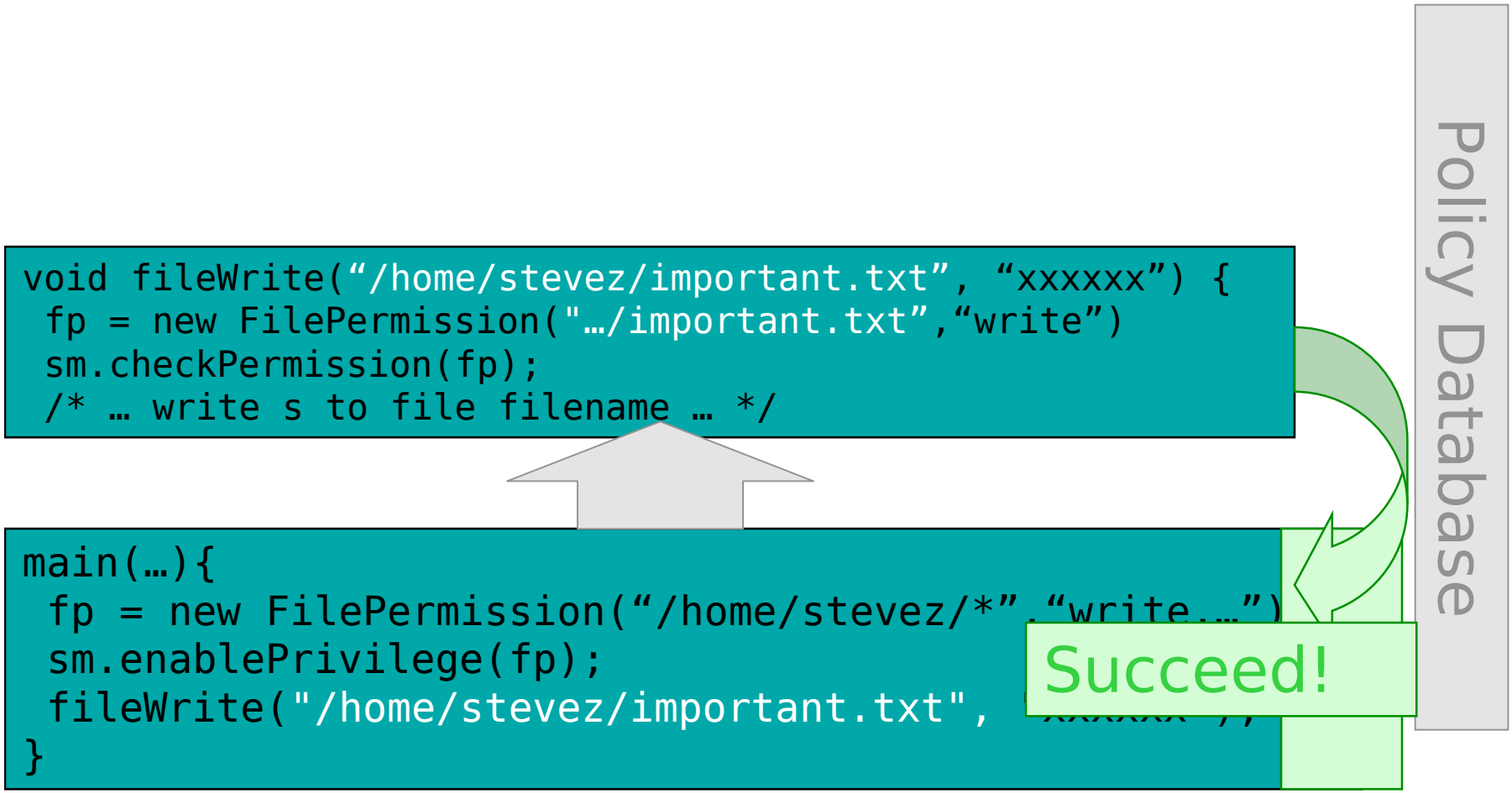
Problem with Stack Inspection

Problem with Stack Inspection



Problem with Stack Inspection

Problem with Stack Inspection



Stack Inspection: Final thoughts

- Question: How does taint tracking relate to this problem with stack inspection?

- Related Papers (not required reading):
  - A Systematic Approach to Static Access Control
    François Pottier, Christian Skalka, Scott Smith
  - Stack Inspection: Theory and Variants
    Cédric Fournet and Andrew D. Gordon
  - Understanding Java Stack Inspection
    Dan S. Wallach and Edward W. Felten

Covert Channels & Information Hiding

- A covert channel is a means by which two components of a system that are not permitted to communicate do so anyway by affecting a shared resource.

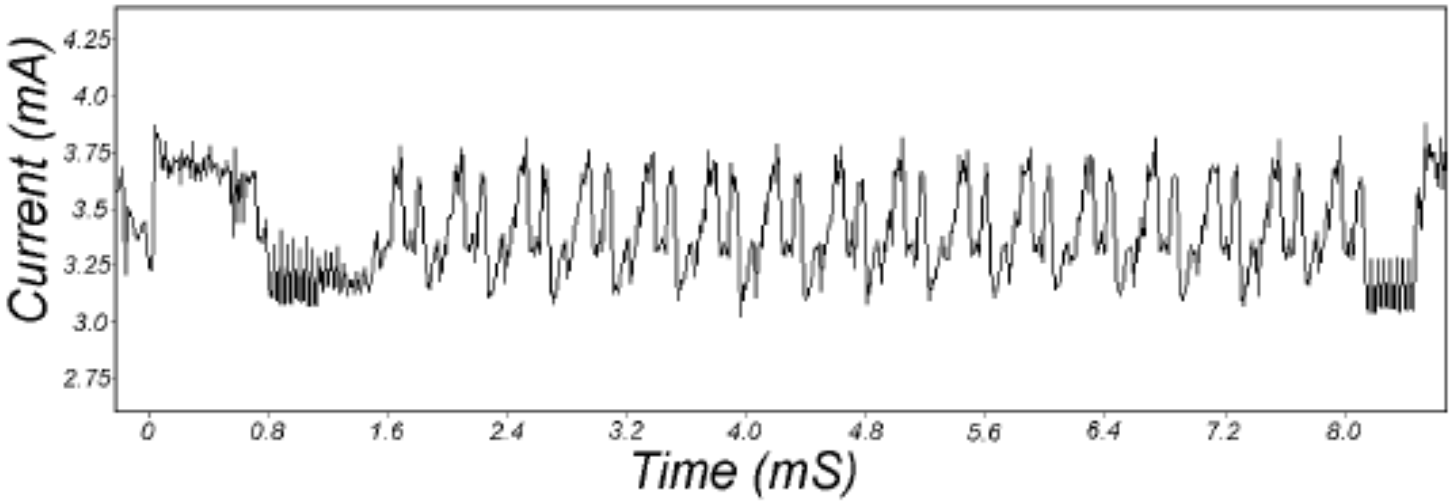
- Information hiding: Two components of the system that are permitted to communicate about one set of things, exchange information about disallowed topics by encoding contraband information in the legitimate traffic.

- Not that hard to leak a small amount of data
  - A 64 bit encryption key is not that hard to transmit
  - Even possible to encode relatively large amounts of data!

- Example channels / information hiding strategies
  - Program behavior
  - Adjust the formatting of output:
    use the “\t” character for “1” and 8 spaces for “0”
  - Vary timing behavior based on key
  - Use "low order" bits to send signals
  - Power consumption
  - Grabbing/releasing a lock on a shared resource

Differential Power Analysis

- Read the value of a DES password off of a smartcard by watching power consumption!



- This figure shows simple power analysis of DES encryption. The 16 rounds are clearly visible.

TEMPEST Security

- Transient Electromagnetic Pulse Emanation Standard
  - (Or?) Temporary Emanation and Spurious Transmission
  - Emission security (Van Eck phreaking)
  - computer monitors and other devices give off electromagnetic radiation
  - With the right antenna and receiver, these emanations can be intercepted from a remote location, and then be redisplayed (in the case of a monitor screen) or recorded and replayed (such as with a printer or keyboard).
- Policy is set in National Communications Security Committee Directive 4
- Guidelines for preventing EM reception
  - Shield the device (expensive)
  - Shield a location (inconvenient?)

Watermarking Basic Idea

- Pictures, Video, and Sound
  - Human perception is imperfect
  - There are a lot of “least significant bits”
  - Modifying the least significant bits doesn’t change the picture much

(R,G,B) = (182,54,89)

(R,G,B) = (182,54,90)

- Encode a signal in the least significant bits.

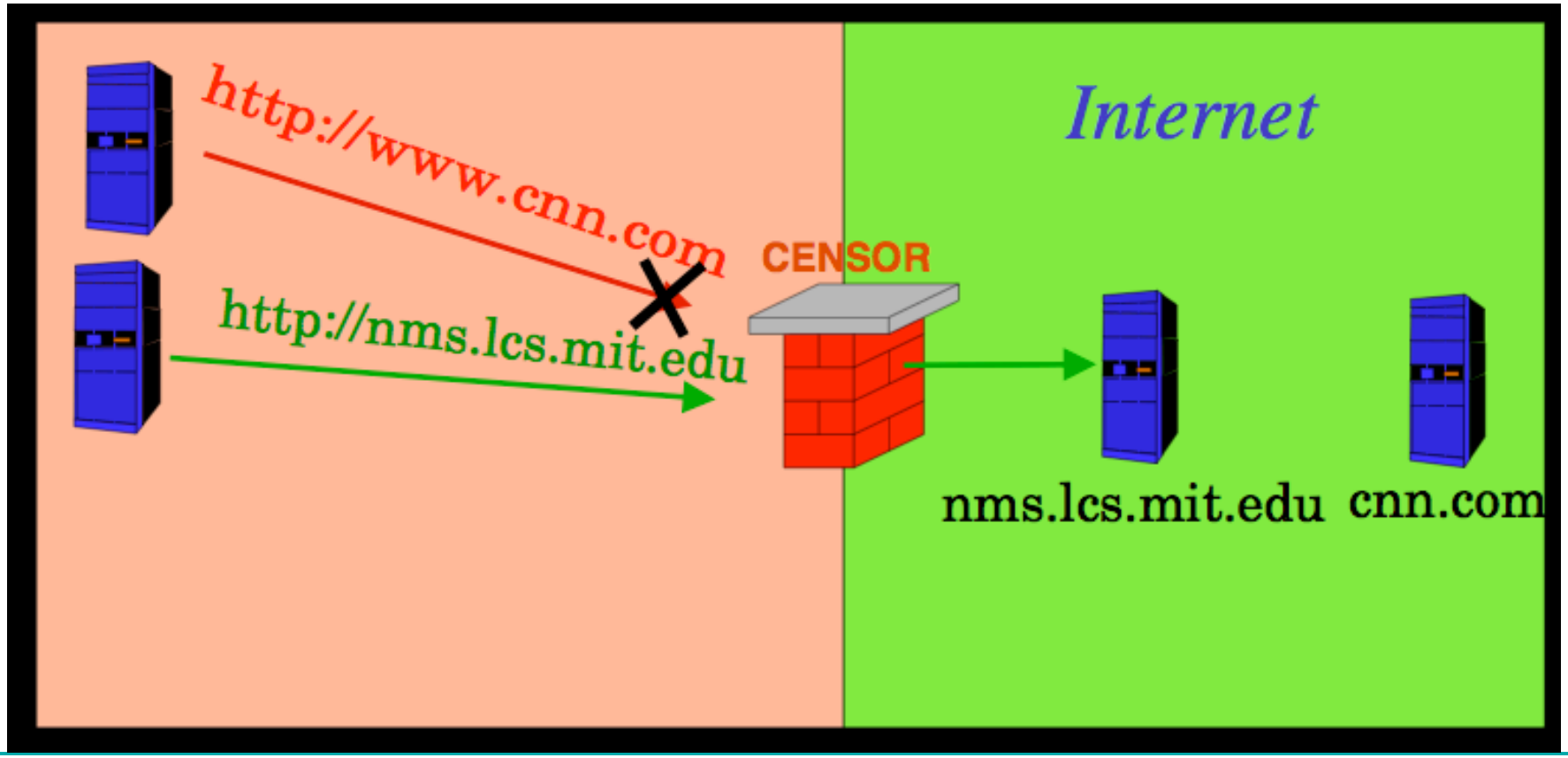
Watermarking Example

Original Image

Watermarked Image

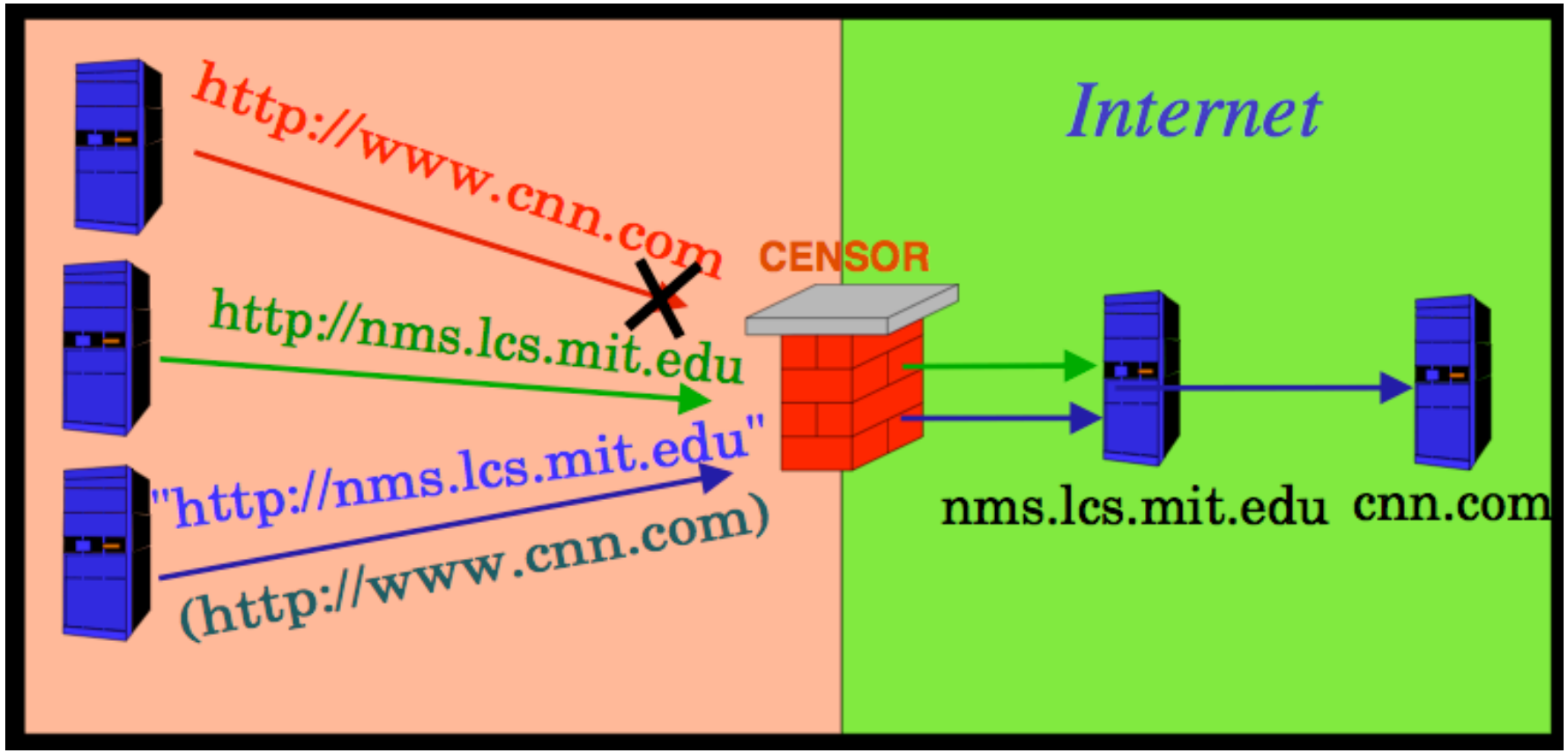
Example application: Infranet

- Infranet: Circumventing Censorship and Surveillance (Feamster et al. 2002)
  - http://nms.csail.mit.edu/infranet

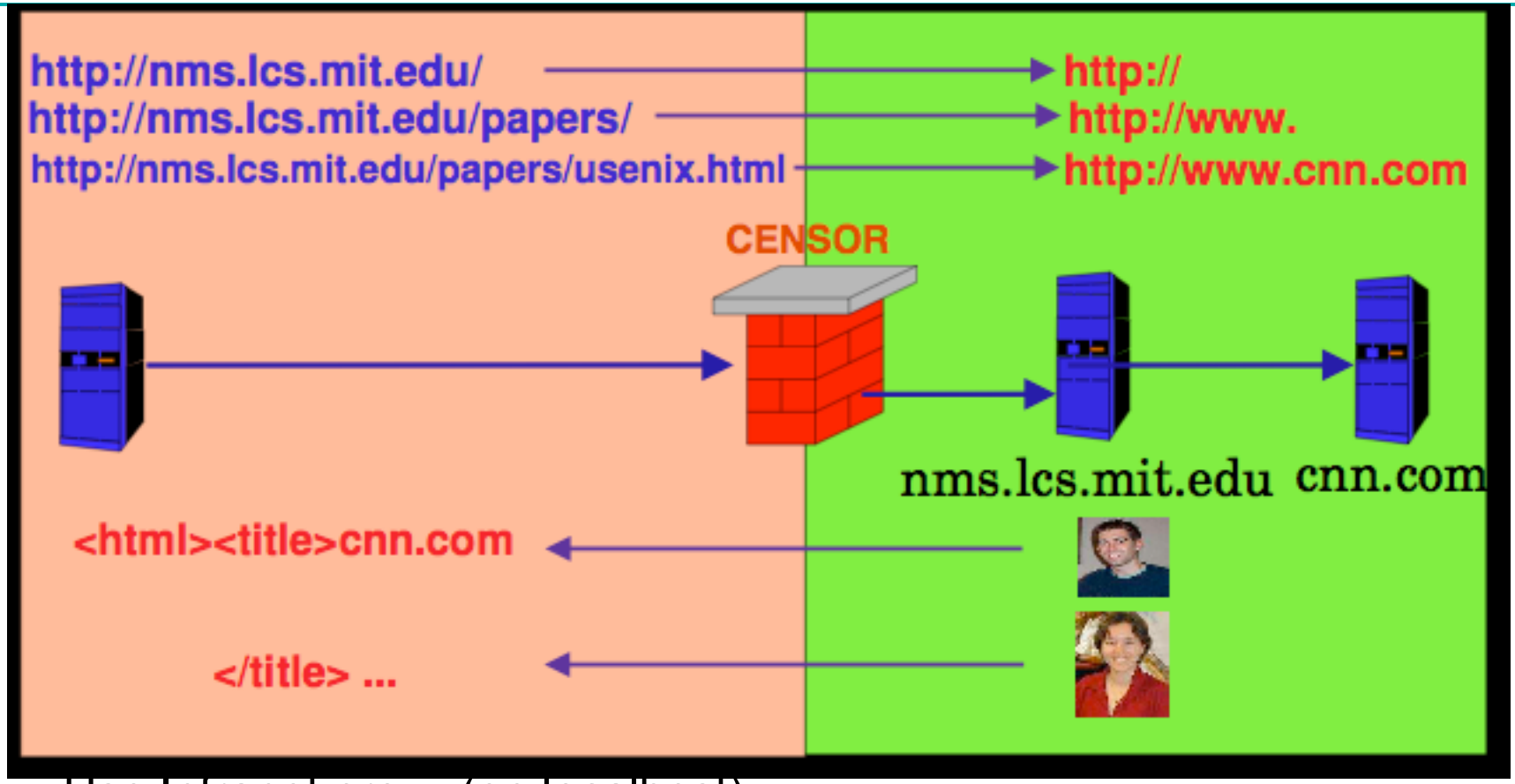


Infranet: Exploit covert channels

- Idea: Tunnel covert HTTP traffic through "legit" HTTP traffic.



How Infranet Works



- Use Infranet proxy (on localhost)
- Upstream request sent in sequence of HTTP requests
- Downstream reply encoded in images

Defenses for Covert Channels

- Well specified security policies at the human level
- Auditing mechanisms at the human level
  - Justify prosecution if the attacker is caught
- Code review
  - This is a form of audit
- Automated program analysis
  - Type systems that let programmers specify confidentiality labels
  - Transform programs so that both branches of a conditional statement take the same amount of time
  - Disallow branches on "secret" information
- Automated system analysis
  - Monitor http traffic to look for unusual behavior

Specific Countermeasures

- Against timing attacks:
  - Make all operations run in same amount of time
    - Hard to implement!
    - Can't design platform-independent algorithms
    - All operations take as long as slowest one
  - Add random delays
    - Can take more samples to remove randomness
- Against power analysis attacks:
  - Make all operations take the same amount of power
    - Again, hard to implement
  - Add randomness

Question:

- Suppose you have gone through the cost/benefit and risk analysis to determine the securty requirements for a computer system.
- How do you know whether a system meets its security requirements?

- Class answers:

Assurance methods

- Testing
  - Regression testing, automation tools, etc.
  - Can demonstrate existence of flaw, not absence
- Validation
  - Requirements checking
  - Design and code reviews
    - Sit around table, drink lots of coffee, …
  - Module and system testing
- Formal verification
  - Develop a rigorous (mathematical) specification of the system
  - Prove (using tools or by hand) that the implementation meets the specification
  - Time-consuming, painstaking process
  - Has been done for some systems. (See www.praxis-his.com)

Rainbow Series

DoD Trusted Computer Sys Evaluation Criteria (Orange Book)
Audit in Trusted Systems (Tan Book)
Configuration Management in Trusted Systems (Amber Book)
Trusted Distribution in Trusted Systems (Dark Lavender Book)
Security Modeling in Trusted Systems (Aqua Book)
Formal Verification Systems (Purple Book)
Covert Channel Analysis of Trusted Systems (Light Pink Book)
… many more

http://www.radium.ncsc.mil/tpep/library/rainbow/index.html

Orange Book Requirements (TCSEC)

- TCSEC = Trusted Computer System Evaluation Criteria

- Security Policy
- Accountability
- Assurance
- Documentation

- Next few slides: details not important …
  - Main point: Higher levels require more work …, documentation and configuration management are part of the criteria

Orange Book Criteria (TCSEC)

- Level D
  - No security requirements
- Level C For environments with cooperating users
  - C1 – protected mode OS, authenticated login, DAC, security testing and documentation (Unix)
  - C2 – DAC to level of individual user, object initialization, auditing (Windows NT 4.0)
- Level B, A
  - All users and objects must be assigned a security label (classified, unclassified, etc.)
  - System must enforce Bell-LaPadula model

Levels B, A (continued)

- Level B
  - B1 – classification and Bell-LaPadula
  - B2 – system designed in top-down modular way, must be possible to verify, covert channels must be analyzed
  - B3 – ACLs with users and groups, formal TCB must be presented, adequate security auditing, secure crash recovery
- Level A1
  - Formal proof of protection system, formal proof that model is correct, demonstration that impl conforms to model, formal covert channel analysis

Common Criteria

- Three parts
  - CC Documents
    - Protection profiles: requirements for category of systems
      - Functional requirements
      - Assurance requirements
  - CC Evaluation Methodology
  - National Schemes (local ways of doing evaluation)
- Endorsed by 14 countries
- Replaces TCSEC
  - CC adopted 1998
  - Last TCSEC evaluation completed 2000

http://www.commoncriteria.org/

Protection Profiles

- Requirements for categories of systems
  - Subject to review and certified
- Example: Controlled Access PP (CAPP_V1.d)
  - Security functional requirements
    - Authentication, User Data Protection, Prevent Audit Loss
  - Security assurance requirements
    - Security testing, Admin guidance, Life-cycle support, …
  - Assumes non-hostile and well-managed users
  - Does not consider malicious system developers

Evaluation Assurance Levels 1 – 4

EAL 1: Functionally Tested

- Review of functional and interface specifications
- Some independent testing

EAL 2: Structurally Tested

- Analysis of security functions, including high-level design
- Independent testing, review of developer testing

EAL 3: Methodically Tested and Checked

- Development environment controls; configuration mgmt

EAL 4: Methodically Designed, Tested, Reviewed

- Informal spec of security policy, Independent testing

Evaluation Assurance Levels 5 – 7

EAL 5: Semiformally Designed and Tested

- Formal model, modular design
- Vulnerability search, covert channel analysis

EAL 6: Semiformally Verified Design and Tested

- Structured development process

EAL 7: Formally Verified Design and Tested

- Formal presentation of functional specification
- Product or system design must be simple
- Independent confirmation of developer tests

Example: Windows 2000, EAL 4+

- Evaluation performed by SAIC
- Used “Controlled Access Protection Profile”
- Level EAL 4 + Flaw Remediation
  - “EAL 4 … represents the highest level at which products not built specifically to meet the requirements of EAL 5-7 ought to be evaluated.”

    (EAL 5-7 requires more stringent design and development procedures …)
  - Flaw Remediation
- Evaluation based on specific configurations
  - Produced configuration guide that may be useful

National Information Assurance Partnership

Common Criteria Certificate

Microsoft Corporation

The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 1.0) for conformance to the Common Criteria for IT Security Evaluation (Version 2.1). This certificate applies only to the specific version and release of the product in its evaluated configuration. The product's functional and assurance security specifications are contained in its security target. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

Product Name: Windows 2000 Professional, Server, and Advanced Server with SP3 and Q326886 Hotfix
Evaluation Platform: Compaq Proliant ML570, ML330; Compaq Professional Workstation AP550; Dell Optiplex GX400; Dell PE 2500, 6450, 2550, 1550
Assurance Level: EAL4 Augmented

Name of CCTL: Science Applications International Corporation
Validation Report Number: CCEVS-VR-02-0025
Date Issued: 25 October 2002
Protection Profile Identifier: Controlled Access Protection Profile, Version 1.d, October 8, 1999

Director
Information Technology Laboratory
National Institute of Standards and Technology

Information Assurance
Director
National Security Agency

Is Windows is “Secure”?

- Good things
  - Design goals include security goals
  - Independent review, configuration guidelines
- But …
  - “Secure” is a complex concept
    - What properties protected against what attacks?
  - Typical installation includes more than just OS
    - Many problems arise from applications, device drivers
    - Windows driver certification program