

CS 671: Secure Computing in the Post-PC World

Thu D. Nguyen

Fall 2000

A Snazzy Quote

National and economic infrastructures are coming to depend on networked information systems, or NISs. These systems must be *trustworthy* – do what users and operators expect (and not something else) despite environmental disruption, human user and operator errors, *attacks by hostile parties*, and system design and implementation errors.

– Schneider, Bellovin, and Inouye, 1999.

Thu D. Nguyen

2

Rutgers University

Goal

- Read enough papers to get good background on security
 - Note that, for us, security \neq cryptography
- Think about research in security (or trusted computing)
- Start some research through projects

Thu D. Nguyen

3

Rutgers University

Administration

Administrative Details

- Class time
 - Tuesdays 12:30-2:30
 - Can do 11:30-1:30 or 12:00-2:00
- Office hours
 - Thursdays 10:30-12 (?)
- Monitor the following web site closely
 - <http://www.cs.rutgers.edu/~tdnguyen/classes/cs671/>
 - Will have sort of bulletin board (or mailing list)

Thu D. Nguyen

5

Rutgers University

What to Expect

- 2 papers per week (occasionally 3 when one or more papers are “light”)
- 1-2 presentations per student
- Project (possibly short presentation at end of seminar)

Thu D. Nguyen

6

Rutgers University

Weekly Presentations

- We're only doing 2 papers a week
 - Everyone should read the papers carefully
 - Presenter must:
 - Prepare "real" presentations
 - Should try to find additional material related to paper to enhance presentation
 - Meet with me by Thursday of previous week to go over presentation
 - Idea is for you to get practice giving presentations

Thu D. Nguyen 7 Rutgers University

Grading

- This is a seminar so grading is not particularly harsh
- On the other hand, grades won't be entirely free
 - 30% presentation
 - 30% participation
 - 40% project

Thu D. Nguyen 8 Rutgers University

Project

- There's no "canned" project
- Likely, I'll have a small list of possible projects
- You're responsible for defining a project
 - Of course, I'll help
- Project can be set in larger context of *trusted computing*

Thu D. Nguyen 9 Rutgers University

Related Reading Group

- Availability and Consistency in Internet Services
 - Tuesdays, 3-4pm, CoRE A
 - <http://www.cs.rutgers.edu/~rmartin/teaching/fall00A/index.html>

Thu D. Nguyen 10 Rutgers University

Trusted Computing

Context

- The computing landscape is changing
- Old model:
 - PC at home
 - LAN at work with client/server computing
- New model:
 - Internet services
 - Access services through PCs, public kiosks, PDAs, cell phone, etc.
 - Still may have elements of old model for a long while

Thu D. Nguyen 12 Rutgers University

What We Want

- We're trusting more and more of our daily life to this new computing infrastructure
 - Electronic banking
 - Electronic stock trading
 - On-line medical databases
 - Email, daily schedule, etc.
- We want to be able to *trust* our computing infrastructure
 - Want our computing infrastructure to do what we want (no more, no less) when we want it done

Thu D. Nguyen 13 Rutgers University

Trustworthiness

- Trustworthiness encompasses many fields
 - Correctness
 - Reliability
 - Survivability
 - Security and Privacy
- Example
 - I'm not sure about the accuracy of this story but, nevertheless, I'm telling it to make a point
 - Recently, Microsoft put a machine running Windows 2000 on the net and challenged hackers to break into it
 - Before hackers can try, the machine crashed and stayed down for quite a while
 - The point: you can have perfect security if you don't let anyone access your computing resources ☺

Thu D. Nguyen 14 Rutgers University

Back to Project

- In this seminar, we are going to concentrate on the security aspect of trusted computing
 - "Security is concerned with ensuring that a system resists potentially correlated events (attacks) that can compromise the secrecy, integrity, or availability of data and services." – *Trust in Cyberspace*.
- However, projects in the larger context of trusted computing is acceptable
 - Program correctness
 - Fault-tolerance/availability

Thu D. Nguyen 15 Rutgers University

Topics

- Cryptography and Authentication
 - Our focus is NOT on cryptographic techniques but they are a fundamental component of building secure systems so we need to understand a little about how they are used
- Access control
- Dealing with denial-of-service attacks
- Safety and security for mobile code
- Secure access from untrusted access points
- Intrusion detection
- Controlling interactions between heterogeneous distributed agents
- More to come ... suggestions?

Thu D. Nguyen 16 Rutgers University

Why Security?

- Right now, achieving high availability is probably more troublesome than achieving high security
 - Example: Britanica Web site
- However, security is a rising concern
- As we trust more and more of our critical data and transactions to the Internet, we can expect more attacks
 - Example: Yahoo DoS attack
 - Other examples of break-ins to both military and non-military systems are given in Chapter 1 of *Trust in Cyberspace*

Thu D. Nguyen 17 Rutgers University

Security Has Gotten "More Interesting"

- Historically
 - "Practical security" was limited to access control on time-sharing systems
 - DoD security, which is mostly "how do I keep secret information secret?"
- Now
 - Computing infrastructure includes many different devices – PCs, PDAs, cell phones, public kiosks, etc.
 - Economics dictate that computing infrastructure be built from COTS components
 - "To a first approximation everything is becoming interconnected." – *Trust in Cyberspace*
 - Mobile code
 - Distributed heterogeneous agents

Thu D. Nguyen 18 Rutgers University

Some Background

- **Definition**
 - “Security is concerned with ensuring that a system resists potentially correlated events (attacks) that can compromise the secrecy, integrity, or availability of data and services.” – *Trust in Cyberspace*.
- **Security has typically been subdivided into three areas**
 - Preventing the disclosure of information (disclosure)
 - Preventing the modification or destruction of information (integrity)
 - Preventing denial-of-service (denial-of-service)
 - Does “preventing denial-of-service” = availability?
- **Is this categorization complete?**

Thu D. Nguyen 19 Rutgers University

Terminology

- **Threat**
 - A potential attack that someone may want to initiate against a computing system
- **Vulnerability**
 - A flaw in a computing system allowing a threat to be carried out
- **Attack**
 - ... well, this is sort of obvious, right?

Thu D. Nguyen 20 Rutgers University

Implementing Security

- **Implementation of security is typically split into two parts**
 - Mechanisms to support security
 - Policies that should/must be enforced
 - (519 students, sounds familiar?)
- **Trusted computing base**
 - Combination of hardware/software that is trusted to enforce the desired security policies
 - Example: the OS and hardware is typically the trusted computing base of a multi-programmed system
 - Security/trust has to start from somewhere
- **Trusted agent**
 - In untrusted distributed environments such as the Internet, security/trust often arise from trusted agent – e.g., public key server

Thu D. Nguyen 21 Rutgers University

Cryptography

- **Cryptographic methods are pretty fundamental to implementing security**
 - Certificates
 - How I can prove I'm Thu (someone you trust says that I'm Thu)
 - How I can prove that I have certain access rights
 - Digital signatures
 - How I can prove that some information you got from me has not been altered in any way
 - Encryption/decryption
 - How I can protect secret/private information from others
- **We are going to assume the existence of strong cryptographic methods**

Thu D. Nguyen 22 Rutgers University

What Do We Need to Worry About?

- **Building Trustworthy Systems: Lessons from the Public Telephone Network and Internet – Schneider, Bellovin, Inouye, 1999.**
 - **Environmental disruptions**
 - Link failures: “backhoe fading”
 - Congestion
 - **User and operator errors**
 - In the past, some OS'es were shipped with a standard root password – guess what happens?
 - **Hostile attacks**
 - PTN: routing attacks, database attacks
 - Internet: DNS attacks, routing attacks, denial-of-service attacks

Thu D. Nguyen 23 Rutgers University

Open Source More Secure?

- **An overwhelming majority of security vulnerabilities are caused by “buggy” code**
- **While this is in the realm of software engineering (which is a part of trusted computing), we must be especially concerned with the correctness of security mechanisms**
 - Can perhaps spend more resources to make sure that this code is correct
- **An interesting approach: OpenBSD's “proactive auditing”**
 - <http://www.openbsd.org>
- **Does open source help?**
 - Does more eyes help to find/fix security bugs?
 - Some interesting opinions on the class reading list

Thu D. Nguyen 24 Rutgers University