

# Authentication in Distributed Systems Part I

CS262  
April 14, 2008

# Administrivia

- Course Evaluations
  - Open next week
  - Please fill them out
- Programming assignments
  - Assignment 1 ends tomorrow, 2 next week
  - If you are having trouble, talk to me

# Administrivia

- Tomorrow is the last day for programming assignment I
- First project presentations are in two weeks
- Second Exam a week from Wednesday

# Why Theory?

- Allows us to formalize our intuitions
  - We think we know what we mean
  - This lets us check
- Theories are precise
  - If we agree, we know what we are agreeing to
  - We can work out the implications

# The Theory

- Syntactic
  - Tells you what can be said
  - Tells you the axioms and implication rules
  - Gives an intended meaning
- Semantics
  - Gives a meaning
  - For each syntax rule, an interpretation rule

# Basic Notions

- Principal
  - Source of a request
  - What we grant access
- Requests
  - Do something, give access to something
- ACL
  - Specifies who can access
- Trusted computing base

# The Goal

- An action,  $s$ , can occur when
  - $A$  says  $s$ , and
  - $A$  is in the ACL for the resource needed for  $s$
- $A$  is generally a person, a group of people, or a role
- Only channels directly say anything

# Principles

- People, Machines
- Roles
- Sets of principles
  - Services
  - Groups
- Channels

# Principals

- The set of principals is defined inductively
  - A set of primitive principals :A, B, C, ...
    - Intuitively, these are all of the entities that can say things
  - If A, B are principals, then so are
    - “ $A \wedge B$ ” (the principal that is both A and B)
    - “A|B” (A quoting B)
- Remember the type...

# Statements

- Inductively defined as
  - A set of primitive statements  $p, q, r, s, s', \dots$
  - If  $s, s'$  are statements, so are
    - $s \wedge s', s \supset s', s \equiv s'$
    - If  $A$  is a principal, then “ $A$  says  $s$ ” is a statement
    - If  $A$  and  $B$  are principals, then “ $A \Rightarrow B$ ” is a statement ( $A$  speaks for  $B$ )
- Some standard things are missing...

# Semantics

- Statements are interpreted as true or false
- Principals are interpreted as a set of statements
  - Think of the set as all the statements made by that principal
  - $\text{Int}(A \text{ says } s)$  is true iff  $s \in S = \text{Int}(A)$
  - “ $A \wedge B$ ” =  $\text{Int}(A) \cap \text{Int}(B)$

# Axioms

- Basic
  - If  $s$  is an instance of a theorem of propositional calculus, then  $\vdash s$
  - $\vdash s$  and  $\vdash s \supset s'$  then  $\vdash s'$
  - $\vdash (A \text{ says } s \wedge A \text{ says } (s \supset s')) \supset A \text{ says } s'$
  - if  $\vdash s$  then  $\vdash A \text{ says } s$  for all principals  $A$

# Therefore...

- $\vdash A \text{ says } (s \wedge s') \equiv (A \text{ says } s) \wedge (A \text{ says } s')$ 
  - Follows from S1-S4
- $\vdash (A \wedge B) \text{ says } s \equiv (A \text{ says } s) \wedge (B \text{ says } s)$ 
  - Doesn't follow from S1-S4, or even S1-S5
- $\vdash (A|B) \text{ says } s \equiv (A \text{ says } B \text{ says } s)$
- $\vdash A = B \supset (A \text{ says } s \equiv B \text{ says } s)$ 
  - Note- this isn't a wff unless we add a definition of "="

# Speaks For

- We need to add
  - $\wedge$  is associative, commutative, and idempotent
  - $|$  is associative
  - $|$  distributes over  $\wedge$  in both arguments
- We can define “ $\Rightarrow$ ”, or speaks for, as
  - $\vdash (A \Rightarrow B) \equiv (A = (A \wedge B))$ 
    - This can be weakened to A speaks for B for some s

# Which gives us

- $\vdash (A \Rightarrow B) \supset (A \text{ says } s) \supset (B \text{ says } s)$
- $\vdash (A = B) \equiv ((A \Rightarrow B) \wedge (B \Rightarrow A))$
- And, most importantly,
  - $\vdash (A \text{ says } (B \Rightarrow A)) \supset (B \Rightarrow A)$
  - $\vdash ((A' \Rightarrow A) \wedge A' \text{ says } (B \Rightarrow A)) \supset (B \Rightarrow A)$

# Encryption

- Limits the trusted base
  - All intermediaries need not be trusted
- Lets channels be identified
  - Channel with  $s$  encrypted with  $A$ 's key =  $A$  says  $s$
- Without encryption, the system wouldn't change
  - Just be more complex

# Principals and Channels

- You know channel  $C$  is encrypted with  $k$ 
  - How do you find the principal associated with  $k$
- Certificate authorities
  - These are trusted and secure
  - They keep a mapping of keys to principals
  - CA says  $(k \Rightarrow A)$

# Pathnames

- Intuition
  - There will be multiple authorities
  - They will be organized in a tree (hope)
  - We want the least tree for authentication
- Need some way to add this to the logic

# Pathnames

- We add named principals
  - If  $P, N$  are pathname principals, then  $P/N$  is a principal
  - If  $P, N$  are pathname principals, then  $P$  except  $N$  is a principal
- This is a best guess
  - This section is pretty incoherent formally

# Axioms

- $\vdash P \text{ except } M \Rightarrow P$
- $\vdash M \neq N \supset (P \text{ except } M) \mid N \Rightarrow P/N$   
except ‘.’
- $\vdash M \neq \text{‘.’} \supset (P/N \text{ except } M) \mid \text{‘.’} \Rightarrow$   
 $P \text{ except } N$

# Groups

- Groups are principals
  - No key, so they never say anything directly
  - Instead, a set of principals that are members
  - Members speak for the group