Security for the Working Programmer

Adam Martin - ACCU 2005

Should you be here?

- Not if you want:
  - An overview of cryptography
  - A new encryption algorithm
- ...but stay for:
  - A method for implementing security cheaply

Security Primer

- Tools != Security
  - Cryptography
  - Authentication
  - Authorization

Security Primer

- 3 Key Aspects
  - Prevention
  - Detection
  - Response

Security Primer

- If you remember nothing else...
  - Most attacks involve an insider
  - Most breaches use buffer overflow
  - Secure systems do NOT compose securely
  - Security by obscurity is no security at all

Games...

- “Every user is your enemy”
  - Diablo: a disaster
    - Authoritative client, using encryption
  - ...Diablo2?

Diablo2

- “Diablo2 will never be hacked”
- Map hacks
- Item duping
- Item-grab + Heal-auto + Monster-seek bots
- User: trade-mistakes, -timing, -bugs
- User: fake in-game-service provider

Value of Fear

- Security is invisible
- Secure systems don't make money
  - ...how do you get the budget?

My Situation

- CTO: Perplex City
  - 18 months
  - 4 years
  - 9 staff
- Online Game - 50k
  - ... 1 million

My Situation

- Why is Security important to me?
  - Gameserver converts tokens to playtime
  - Lose tokens == lose money
  - Gameserver allow false tokens == ...
  - Gameserver hacked, tokens stolen == ...
  - Gameserver hacked, defaced == look stupid, lose job

My Situation

- Ultimately:
  - Lose or leak info == go out of business

Problems

- No-one knows if secure

Problems

- Can't afford to over-engineer
  - already had c.7 international articles
  - launch deadline approaching
  - finite cash
  - tech == critical path
    - ...security "easy" candidate for eviction!

Problems

- Nature of game: "to hack systems"
  - Beast: hacking puzzle
  - ILB: hacking puzzle
  - Majestic: hacking puzzle
    - ...thanks, Sean + Elan!
    - ...even our own promotional game...

Problems

- Staff and Partners hate encryption, forget passwords
  - No PGP mail
  - Only brutality (BOFH) works
  - OS X + Linux + Windows

Practical Needs

- Need to:
  - Measure Secureness
  - Create *effective* security
  - Save time
  - Make security popular

Measure Secureness

- Quantify impact of changes
- Point to Weakest Link
  - ...often, “forgot to include users as part of the system”
  - ...but: EA controller hack

Create Effective Security

- No expertise; need all the help we can get

Save Time

- FAST
- not on crit path (people, tasks)

Make Security Popular

- Get all staff involved?

Fundamental Problem?

- No idea what we're doing...
- No idea:
  - What we have left to do
  - How long it will take
  - Where it's vulnerable
  - Where we could "save time"

Fundamental Problem?

- ...and everyone else thinks Security is dull
- “...and annoying”

A Simple And Practical Process

- "A quantitative measure of Secureness"
- Core idea: S = I - R
  - I: Insecurity
  - R: Level of Response to Insecurity
  - S: "Secureness"

A Simple And Practical Process

- Simpler than CC
  - takes too long
  - requires expensive specialists
  - results are too verbose

Measuring Insecurity

- Threat Modelling
  - A cracker's specification...
  - ...an inverse SRS

Measuring Insecurity

- Threats / Attacks
  - Independent
  - Concrete
  - Detailed / precise

Threat Models

- Modelling technique:
  - Effectiveness doesn't matter
  - Motivational AND stochastic
  - Technical AND non-technical
  - Reject nothing!

Threat Models

- Effective models are:
  - invented in parallel - separate groups
  - iterative and collaborative - sparks
  - a brainstorming exercise - all POV help
  - easy to read; easy to append to

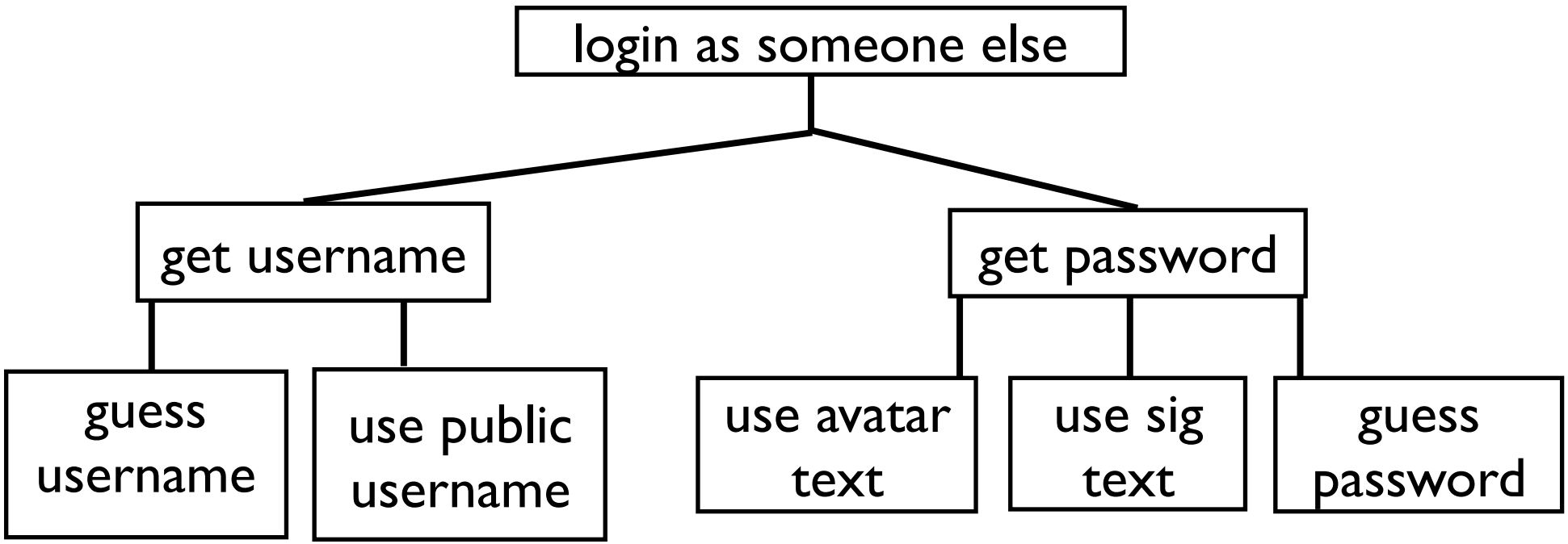
Threat Models

- Bad models
  - long, all-scenario, threats
  - artificial categorization
- Gets messy...
  - e.g. N different ways to guess a password

Threat Models

- Need:
  - for all partial attacks: “Where does this lead?”
  - for all partial attacks: “How can I get to this point?”
- Solution:
  - Attack trees

Attack Trees



Attack Trees

- Benefits
  - compact
  - predictive
  - threat-threat independence
  - divide-and-conquer
  - objective
  - appropriate structure

Attack Trees

- Disadvantages
  - always appear complete
  - lack authoring-tools

Using the Threat Model

- Size approximates I
- Various weighted metrics
  - p(X)
  - p(X | M)
  - `1 / d( X )`
  - a.f.l.(X)

Using the Threat Model

- SRS improvement
- A test plan

Reducing Insecurity

- Security Policy
  - SRS for security
  - Mirrors the Threat Model

Security Policy

- Differences from Threat Model
  - Structure
  - Content

Security Policy

- Policy-writing technique:
  - Explicitly records countering decisions
  - Technical personnel only
  - Specialist knowledge helps
  - Iterate across all threats...methodical

Security Policy

- Bad policy-statements
  - aspirational
  - vague
  - groundless

What Next?

- Disseminate Security Policy
  - Understanding and acceptance...
- Programmers revise Threat Model
  - Minimum acceptable action...
- Periodic re-evaluation of SP
  - PM best practice...

Summary

- "Security Target"
  - Combination of TM and SP
  - Made of "living" documents
  - Quantifies "secureness"
  - Cheap to add threats and ignore them

If you remember nothing else...

- Most attacks involve an insider
- Most breaches use buffer overflow
- Security by obscurity is no security at all
- Secure systems do NOT compose securely

More Games...

- Trusted client disasters
  - Ultima Online (light hack)
  - Counter Strike (wall hack)
- Wrong problem
  - Dupes and inflation
  - Most cheats are scams