

Thinking About Security

September 29, 2004

Ryan Matteson

ITS Office of the CIO – Security Assurance

Introduction: My Role

- OCIO/Security Assurance: identifying security needs and measures to meet those needs
- Work with campus Information Security Officer, Vicki Stover, who manages the Information Security Program.

Also: enterprise systems architecture, software development and consulting

Agenda

The questions I hope to answer:

- What is security?
- Why does it matter?
- How can we think about security in a productive way?
- How do campus password practices fit this way of thinking?
- Additional questions you may have.

What is security?

- Security is freedom from risk or danger.
- Risk can never be completely removed, but it can be lessened
- Today we will focus on risks related to information systems.

Why does it matter?

- At Cal Poly we have many valuable assets, and some of these are held in or controlled by information systems.
- Compromises of these assets cost us (time, money, reputation, legal compliance)
- Many of you rely on information systems, and some work with sensitive information.

How do we think about security?

- Security can be:
 - A **process**: ongoing effort towards a goal
 - An **enabler**: making things practical by lowering risk (it's not about creating inconvenience).
 - **Risk management**: allocating resources towards the effort, based on analysis of dangers or costs
- All of us share some responsibility for security (of ourselves, and of Cal Poly).
- It's a balancing act

How do we think about security?

- In information systems, the primary goals are C I A
 - Confidentiality: enforce secrecy, protect privacy
 - Integrity: protect accuracy/reliability
 - Availability: prevent disruption of service

What about passwords?

- Passwords can *provide all three*: confidentiality, integrity, availability
- To be effective, we must protect passwords from threats
- Following good password practices is a way for you to help improve security – which benefits you and the University.

Threats to Passwords

- Guessing
- Disclosure
- Sharing
- Reuse

Threat: Guessing

- Passwords must be difficult to guess; they must include many different characters and not be based on words
- How ITS is helping: the Password Manager available at my.calpoly.edu displays and follows rules for creating passwords which are difficult to guess.

Threat: Disclosure

- Protect the secrecy of your password
- No sticky-notes on monitors, please!
- How ITS is helping: single username and password for services
- If you have trouble, call the ITS Service Desk at x-67000 or your local support staff

Threat: Sharing

- Each user should have and use their own password, and not share it with others.
- If someone else has a legitimate need to access a system, help them to obtain their own account following the appropriate process.
 - Note: Department/supervisor access to any employee's account must be authorized in advance and in writing by the appropriate Human Resources office.

Threat: Reuse

- Don't reuse your Cal Poly password in other contexts, such as non-University web sites.
- We can protect your password when it is used within Cal Poly systems -- but we can't protect it if you share it with xyz.com!

When In Doubt

- Don't collect information you don't need – especially if it's personal in nature.
- Be sure to protect any information you collect.
- When in doubt, please contact Library technical staff or ITS.

Further reading...

- Cal Poly IT Responsible Use Policy
 - <http://www.calpoly.edu/computing/policy.html>
- Password practices
 - http://helpdesk.calpoly.edu/faq/password_faq.html
- Campus Information Security Program
 - <http://its.calpoly.edu/Policies/isp.pdf>
- Beyond Fear
 - “Thinking Sensibly About Security in an Uncertain World”
 - Bruce Schneier, HV6432 .S36 2003

Contacts

- Immediate threats to safety: call 911
- Violations of campus information or responsible use policies:
abuse@calpoly.edu
- Discussion or questions on information security issues: rmatteso@calpoly.edu