ITPG Proposal [DRAFT V9]

4/20/04 12:22 AM

Project Name:

Building a Trusted Infrastructure: opportunities and issues of digital security on campus.

Project Proposal Originators:

Bill Doering, GGSE

Project Implementers:

Option A - Internal UCSB group
Option B - External consultants
Option C - Combination of Options A and B

Executive Summary:

Our goal is to consolidate UCSB's multiple, independent access and data protection structures into a campus-wide, distributed trust system.

This system should be capable of:

- offering new/enhanced administrative and educational capabilities,
- opening access to buildings, equipment, systems and information,
- augmenting security for the exchange and storage of electronic information,
- saving operational and infrastructure costs,
- generating revenues for UCSB.

Vision:

Snapshots of the campus sometime in the future:

A student enrolls and pays for a class by *digitally authenticating* herself and then typing information into her cell phone. The *phone takes care of all aspects of the transaction*, from communicating the request for payment to her bank, to entering *automatically* all the data requested by UCSB's server.

Another student comes to class on the morning bus as usual, but instead of using a ticket or a special bus pass, he flashes a University *smart card* near the bus's smart card reader and sits down. The *bus recognizes the token* and identifies the student as part of the UCSB/MTD bus rider program. He arrives on campus, goes to the library to pick up a book and flashes *the same card* near the library's card reader to assure the system of his credentials. Finally, before attending a lecture, he walks over to the Rec Cen and with a quick swipe of the same smart card is *granted access* based on his student status.

An alumna of the University wants to review some information from an environmental science class she attended back in 2006 – she searches the school's database, finds the digital transcript, *downloads the data to her PC for her personal use and pays online.*

A system administrator is on a business trip when a campus service goes off-line. He securely *authenticates and authorizes* himself to a secured campus

VLAN from his laptop, then logs in the appropriate server, runs the necessary diagnostics and brings the service back on-line.

A professor seeks frank advice from a Counseling Services specialist via e-mail about a student's behavioral issue. The specialist is happy to help, but doesn't want the sensitive information shared, so she checks the reply as *"confidential".* Rights software ensures that the e-mail cannot be digitally copied, nor forwarded to another individual and will expire after use. She now feels comfortable speaking freely.

This is a vision of a possible future for UCSB: of a campus-wide, user-friendly and secure network environment populated by responsible users with access to helpful services and to physical infrastructure.

ADVANTAGES of a trust system.

Using a simple, unified trust infrastructure for the input, exchange and storage of valuable or confidential information we can massively improve the efficiency of the campus and offer a host of new opportunities. A sample of the types of advantage a trust system offers follows.

- a tamper-resistant campus network environment
- reliable authentication of a person's identity, easy access to buildings, equipment, systems and information using a single smart card or cell phone
- automatic form filling and data entry
- transactional security
- revenue-generating opportunities from the distribution of valuable data
- time and cost savings
- confidentiality and privacy management
- improved virus and worm protection
- secure boot
- curtained memory
- secure e-mail
- secure document management
- spam isolation
- secure streaming video distribution and caching
- key transfer management between devices
- automatic patching capabilities

Yet the technology to fulfill this kind of vision isn't some futuristic fantasy to look at in 2006 or later. It is becoming available now. It is inexpensive. It is extremely secure. And it is enormously capable.

This proposal describes the access and data protection issues we currently face on campus, and it discusses how we can address them by introducing this type of new, trust infrastructure. Finally, it proposes a methodology for incorporating such a system into our network.

Problem Statement:
There are at least two ways to look at access and data protection issues on campus:

» Looked at from an individual project viewpoint, UCSB faces numerous access issues and challenges with the integration, standardization, interoperability and security of its information, computers, servers and network infrastructure.

How does the network administrator protect the system from viruses and worms? How does a residence hall allow only authorized students to gain entry and later identify their meal plan? How do students identify themselves as enrolled to gain access to the RecCen, information systems, 24-hour access labs? How do organizations identify and share information about students without compromising their privacy? How can Facilities Management cost effectively ensure the security of buildings when master keys are lost? How does UCSB ensure that confidential data isn't harmed? If desirable, how do departments disseminate lectures over the network without discounting professors' and the University's ability to retain their interest in the information?

EXAMPLES.

Campus access systems:

- Parking Services uses a smart card and a magnetic stripe card,
- KITP uses a magnetic stripe card for physical access,
- The UCEN has an Access card for debit transactions, Housing's meal plan, ID, etc.,
- Cheadle hall has RF-enabled smart cards for access,
- The Star laboratory in Ellison uses biometrics for access,
- Bren hall uses biometrics for access,
- Campus wireless network access uses a multi-database authentication system,
- Students must obtain and use stickers on a laminated card for use of certain services,
- Student Affairs hopes to implement a NEW student ID card in Fall of 2004,
- Housing is designing a credential based system for residence halls,
- The Library is looking for an integrated system for access, ID, photo-copying and circulation,
- Facilities has just developed a "Campus Standard and Design Criteria" for access control system software.
- Workstation and servers are generally accessed with passwords.

Project managers have answered each of these questions individually with imagination and wisdom. But the collective consequence is that the campus has developed a variety of solutions to similar problems, has deployed systems and equipment that resist integration, and continues to duplicate work at the cost of much effort and expense.

» Yet, considering these apparently diverse problems from a campus-wide perspective we appear to face two principal issues:

1. *How do we protect the integrity of valuable and confidential information as it is input, used, stored and transferred both within the campus network and beyond?*
2. *How do we establish sufficient confidence in a person's identity that we can grant them an appropriate level of access to computing systems or campus locations?*

These issues are related: you cannot have a secure environment without having some assurance of the reliability of those inhabiting it; and you cannot have confidence about a person's reliability without some assurance that the environment they are inhabiting is secure.

We propose to address this shared issue of trust assurance in an organized and methodical fashion.

Solution:
In the past, many who have imagined a solution to the problems of access and data protection have, as a result of their experiences, sensibly learned to approach the subject with considerable caution. In the face of the blizzard of issues and costs associated with developing a robust infrastructure from scratch, they discovered an unbridgeable gap between vision and reality. Simply put, the existing architecture didn't work.

The result was that security was focused at manageable targets – servers and network perimeters, but the network of distributed devices was treated as, essentially, unregulated and untrustworthy. The secured targets were still vulnerable as they interacted with a hostile environment full of piracy, harmful worms and prolific viruses.

The new generation of trusted computing networks and distributed devices are designed to organize and resolve many of these issues. The basic principle of this type of structure is that, if you can provide a secure space within users' PCs (or other types of digital equipment) then you can leverage that to do a number of

things – identify the machine and its user, store and manage valuable data, run programs securely and protect them from some kinds of attack, keep and manage encryption keys. Essentially what this achieves is an extension of trust into users' devices at the edge of the network.

Companies like IBM, HP, Intel, AMD, National Semiconductor, Infineon, Atmel, Microsoft, Nokia, Sony and Sun have over the last couple of years invested billions of dollars in bringing to market a new generation of trustworthy systems and devices (see Appendix for some examples). It is only recently that we have begun to see the potential of these advances.

The new trust systems are based on an infrastructure of tamper-resistant devices (PCs, cell phones, credentials, smart card readers, personal digital assistants etc.), secure servers, and a floating trust management system that knits the different parts of the system together.

1. Tamper-Resistant Devices

   In order to create more robust security in devices, many elements of the architecture have been and continue to be redesigned. Intel and AMD have recently developed new CPUs, Microsoft has been refashioning its OS, companies like Atmel, National Semiconductor and Infineon have introduced a piece of hardware called a Trusted Platform Module to encrypt and protect data, Phoenix Technologies has modified the BIOS. The result is that the security of devices will be considerably more robust, from boot to operation.

   As Microsoft describes it, there will be four key elements in a trust architecture:

   a. Strong Process Isolation
      The protected operating environment isolates a secure area of memory that is used to process data with higher security requirements.

   b. Sealed Storage
      This storage mechanism uses encryption to help ensure the privacy of data that persists on the hard disk of trusted computers.

   c. Attestation
      This occurs when a piece of code digitally signs and attests to a piece of data, helping to confirm to the recipient that the data was constructed by a cryptographically identifiable software stack.

   d. Secure Paths to the User
      By encrypting input and output, the system creates a secure path from the keyboard and mouse to trusted applications and from those applications to a region of the computer screen. These secure paths ensure that valuable information remains private and unaltered.

2. Secure Servers

   (More research needed here)

3. Floating Trust Management System

   In order to knit together the various parts of the trust network, it will be necessary to manage and protect the flow of data as well as the infrastructure. The first trust management systems are available in the marketplace, and contain many features that are crucial. Here's a description of one system:

   a. Document Manager
      Document Manager provides a straightforward way for business users to incorporate file and folder encryption for their sensitive documents and files.

   b. Privacy Manager
      Privacy Manager secures private and sensitive information using the TPM and simplifies Internet use and password-based login.

   c. Digital Signature
      Digital Signature product facilitates the use of digital certificates with a simple point-and-click signing ceremony.

   d. Security Auto-update
      Security Auto-update ensures that your trusted applications are always up-to-date with the latest available improvements.

   e. Trust System Launch Pad
      The Trust System Launch Pad is the central location for accessing your TPM-enabled applications. Easily launch your trusted applications, check for updates or download newly available trusted applications. New trusted applications are automatically added to the Launch Pad.

   f. Key Transfer Manager
      Key Transfer Manager (KTM) is a key archive system for end-users and enterprises that need a simple, yet fully featured method to securely archive, restore and transfer keys having migratable properties that are secured by the TPM. KTM provides a reliable and convenient key archive system for trusted platforms.

The sum total of these changes will be a considerable improvement in the function of the campus' network. **The trust infrastructure offers**:

- A parallel, tamper-resistant campus network environment.

  As the system is operated by a central trust management system, integrated through the trusted nexus and secured by hardware in the device nodes, the campus network now provides a secure space for the storage and exchange of valuable and sensitive data. It does not replace the existing network, it operates alongside it, extending trust out to the

user's device. To add to the assurance that any particular system is secure and the user is who they say they are, the BIOS will boot in secure mode and biometric mechanisms may be added.

- Reliable authentication of a person's identity and easy access to buildings, equipment, systems and information, using a single smart card or cell phone.

  Because the system focuses on authenticating a person's identity at enrollment and then provides them with a robust, universal token (e.g. a campus-wide smart card or cell phone) for all their campus attestation needs, UCSB may allow appropriate levels of access easily to every user. This will also make information or identity theft extremely difficult.

- Automatic form filling and data entry.

  A user may maintain a single, secure list of their confidential information in their device. The University would request permission to use this data in order to complete the personal information requirements of each department. Databases could be updated automatically.

- Transactional security.

  Because the system is extremely tamper-resistant, relatively inexpensive to operate and user authentication is robust, UCSB (as well as banks and others) may be willing to use the trust network to do sensitive and valuable transactions. Risks and costs of error, data theft or transactional repudiation are minimized in this environment.

- The mitigation of numerous malicious code issues

  Secure authentication of information senders, process isolation and automatic patch updates, will render viral e-mails traceable to their source and/or isolated from sensitive or valuable portions of the system. New e-mail and instant messaging software will offer better file attachment handling and increased customer control over downloads of external content.

- Revenue-generating opportunities from the distribution of valuable data.

  UCSB produces an enormous amount of valuable information annually, in the form of lectures, books and films. Suitably and cost-effectively arranged and presented, much of this data can be used to generate revenues via streaming and caching through the worldwide trust network.

- Time and cost savings.

  The repetition currently engendered by repeating similar tasks on an individual project basis will be curtailed, allowing the redeployment of staff into productive educational or revenue-generating projects.

- Confidentiality and privacy management.

  A number of factors contribute to a climate of confidentiality and user privacy protection: ownership of a user's data by the user themselves and its containment within sealed storage; permission software controlling its use by third parties; knowing authoritatively whom you are communicating

with; the creation of campus-wide policies to protect privacy; the use of a privacy information management system. A user will be able to choose different types of disclosure about themselves – from remaining anonymous to establishing their identity beyond a reasonable doubt. They will be able to choose to use the system, or they may opt out altogether and avoid the advantages the system confers.

By defining and deploying an organized security structure that takes advantage of features of this kind, we will be creating a tremendous resource: a single, campus-wide, tamper-resistant access system that will save money, create a host of valuable opportunities, and that will allow UCSB to re-allocate resources, promote education and generate revenues.

Project Beneficiaries:
The students will be the primary beneficiaries because they will benefit from a standardized, ubiquitous approach to the protection and use of valuable and confidential electronic information.

The faculty and staff will find the system offers greater flexibility in communicating with students, and conducting University business by using new features such as secure information distribution and confidential e-mail.

Facilities will benefit from long term cost savings.

The OIT, NOC and information technology groups will benefit from having a standard way to handle authentication/authorization other than passwords.

The campus as a whole will benefit from creating a new source of potential revenue from the distribution of its intellectual property in a condition that assures its protection. UCSB will be able to leverage its connections with alumni, donors, businesses, and indeed, anyone interested in learning, to create real-time relationships and generate revenues, without a costly investment in a distribution mechanism.

Project Summary:
With this model in mind, we suggest the following approach.

First, we will create a Feasibility Study Group and perform a Feasibility Study that:

A. Identifies the full range of campus security issues, as well as, the current projects and future needs of campus stakeholders. Working with campus committees (i.e. ITPG, AuthDir, ITPG-SecWG) to develop standards,

practices and campus coordination will be essential for the project to succeed.

B. Defines a technology structure capable of accommodating these needs. This section of the Feasibility Study will have two primary objectives:

   (i) To understand the complex elements that would provide the security and flexibility we need. (See Appendix - Principal features)

   (ii) To stay current with technical developments, industry roadmaps and institutional issues. This could be accomplished by becoming a member of TCG, and/or sponsoring a seminar or speaker series, and/or working with a consultant.

   (We will not define the technical specifications of an integrated hardware and software system from scratch. Organizations like the Smart Card Alliance, Finread and the Trusted Computing Group - founding members: Intel, Microsoft, HP, IBM, AMD, Sun, Sony - are doing this.)

C. Outlines an approach to switch from legacy systems to trusted systems, manages that switch, and defines employee training needs.

D. Describes the likely costs and benefits of the structure to UCSB.

By performing this feasibility study we can strategically plan and define a suitable distributed digital trust system for the University.

Second, we will beta-test the solution that we believe best suits our needs. We will also identify additional applications of the system during this process.

Third, we will evaluate the results of our work to this point and an evaluation committee will make the decision whether to proceed.

Fourth, if assent is given, we would write an ITPG implementation proposal which would describe and establish the implementation of the trust infrastructure, and required campus standards and practices.

Fifth, if appropriate funds, as identified by the feasibility study, are allocated we would convert the Feasibility Study Group into a Deployment Management Team, and begin deployment of the trust infrastructure. The implementation will likely take place in three stages (see Appendix - Product Categories for further detail):

(i) Secure Infrastructure Deployment

To deploy basic security services in order to protect individual devices and create a campus-wide trust information infrastructure. Legacy systems will necessarily co-exist during this stage and will only gradually be phased out.

(ii) Transaction Execution

To allow the exchange of valuable data between devices.

(iii) Application Development

To develop or incorporate new capabilities once we are familiar with the basic operation of the system.

UCSB Visionary Requirements:
Senior offers would need to endorse this proposal and mandate that any guidelines, standards and implementation recommendations are adhered to.

Matching Opportunities:
We have identified some important near-term issues –

Facilities Management is currently deploying a credential-based building access system based on a published campus standard access control system. Facilities has invested in a software system named "Ready key Pro" from Bosch. They also have implemented a backend SQL database that the Ready key Pro software interacts with. This software is interoperable with a variety of hardware (readers, credentials, etc.) and vendors. They are also currently managing the creation and distribution of credentials for staff and faculty.

The UCEN is currently charged with the management and distribution of the Access card for students. Based on the UCEN's historical experience with card-based systems we have a potential partner with detailed knowledge of the implementation issues. For example, to avoid a wholesale re-investment of their point of sale (POS) system a new card technology must integrate with their POS system. We also can benefit from their intimate understanding of the implementation costs associated with card-based technology. For example, we know that the initial investment in credential tokens will be a major expense and that card replacement must be addressed. Additionally, we expect to have annual staff costs to manage the creation, replacement and troubleshooting of credentials. The UCEN has suggested that with funding they could be the distribution point for students, staff and faculty.

The ongoing UCSB Directory Project has recently purchased Oblix NetPoint software that leverages the valuable collection of information in the campus LDAP directory. This software helps us build an identity management system

that is an essential component of a trust system AND benefits from the security such a system could provide.

Student Affairs would like to implement a NEW student ID card for Fall 2004. It would be essential that this project be able to co-exist with a trust system or ideally be an initial, beta implementation.

Residential Housing also is planning an implementation for Fall 2004 for some type of residential ID card system. Again, it is essential that this project be able to co-exist with a trust system or ideally be an initial, beta implementation.

Project Timeline:
The project should develop along the following timeline:

1. UCSB Feasibility study — By End of Winter 2004
2. Beta Test — By Spring 2005
3. Evaluation and Decision — Summer 2005
4. Implementation in three stages:
   - (i) Secure Infrastructure Deployment — Summer 2005
   - (ii) Transaction Execution — Winter 2005
   - (iii) Application Development — Summer 2006

Costs and Benefits: Initial Year and Recurring:
The performance of a feasibility study is necessary to assess the likely costs and benefits of a system of this nature. The costs of this study could be handled in three ways:

- **Option A COST** - Internal UCSB group - donated staff time.

  Timeline is likely to be extended significantly, and trust system expertise would need to be gleaned.

- **Option B COST** – External consultant(s) – Estimated $135,000 /yr
- **Option C COST** – Combination of Options A and B

Priority:
This study must be highly prioritized to take advantage of the opportunity and investments of current campus projects and new stakeholders looking to implement parts of a trust system.

Appendix:

Principal features of an effective trust system:

- *Central Trust Management System*

  To ensure UCSB is able to set appropriate policies and manage the campus trust infrastructure.
- *Security*

  To protect keys, OS, memory, inputs, BIOS, etc in individual devices.
- *Operational transparency*

  To ensure the system is easy to use.
- *Interoperability*

  To ensure all parts of the system work together.
- *Adaptability in the field*

  To change security algorithms and applications as improvements emerge.
- *Authentication/Authorization (Attestation of the user)*

  To give access to whomever it is due.
- *Transaction model flexibility*

  To accommodate a range of uses (e.g. subscription, rent, one-time payment, metering)
- *Time recording*

  For instance, to record a time of transaction.
- *Rights management*

  To accommodate different models such as confidentiality, ownership and fair use.
- *User Privacy*

  To give users tools to protect themselves from information abuse and to apply privacy policies to the college.
- *Optional User participation*

  To allow individual users to opt out of the structure (and its benefits) if they wish to.
- *Utility services*

  To manage technical issues such as key recovery in the event of password loss, or data destruction where a machine is stolen.
- *Multiplicity of Applications*

  To allow uses such as Physical Access, Financial Transactions, Privacy Information Management, Network Access, Video Streaming and Caching, Secure E-Mail, Secure Document Exchange etc.
- *Transferable Data*

  To ensure that a user can access information on all their devices (e.g. PDA, cell phone, laptop, SmartCard, etc.)
- *Portability and Communication*

  To allow the user to take their devices with them and connect to the network wherever they happen to be.
- *Location awareness*

  To allow a user to seek help if they are lost or in danger.

Product Categories:
We may broadly characterize trust products into three categories:

(i) **Security Infrastructure Products**
These software and hardware products form the backbone of the trust system. Specialized chips (known as Trusted Platform Modules) in PCs, cell phones, smart card readers or PDAs provide the root of trust, offering public key functions, digital signature, encryption, decryption, initialization and various management functions. A trusted software stack makes the TPM transparent and, with the addition of server-based trust management systems, the structure allows privacy and key transfer management, automatic security updates and secure document exchange.

(ii) **Transactional Products**
These products will make it possible to perform sensitive or valuable transactions online more easily and with greater security.

(iii) **OS and Application Products**
These software products will become available over the next few years once a secure infrastructure is in place. We expect to see enhancements to the OS for Windows (PCs), Linux (Servers), Palmsource (PDAs) and Symbian (cell phones), amongst others. Applications will likely incorporate secure video streaming and caching, secure e-mail, online learning aids, and valuable database structures for the organizing and secure distribution of rich streams of information."

Sources & Resources:
Dan Moody – expert on wide range of Trusted Computing issues.

FinRead specification
http://www.finread.com/spip/index.php

Trusted Computing Group
https://www.trustedcomputinggroup.org/home

UCSB Facilities – physical access spec.
http://facilities.ucsb.edu/standards/division_13.htm

EU report
http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp86_en.pdf

Symbian OS
http://www.symbian.com/technology/standard-java.html

TCG advisor
http://www.internetweek.com/e-business/showArticle.jhtml?articleID=17602156&_requestid=157649

Intel's LaGrande review (with charts)
http://www.extremetech.com/article2/0,3973,1274234,00.asp

Microsoft's NGSCB
http://www.microsoft.com/resources/ngscb/four_features.mspx

IBM
http://www-132.ibm.com/webapp/wcs/stores/servlet/CategoryDisplay?storeId=1&catalogId=-840&langId=-1&categoryId=2049132&trac=1A10SEC00

HP
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=PSD_DD030611_CW01