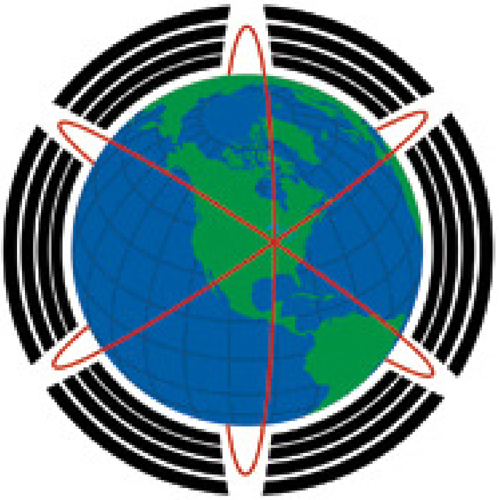
IPRO 310 – FINAL REPORT

Spring 2011



THE OPPORTUNITIES AND CHALLENGES OF MOBILE DEVICES IN THE CORPORATE COMMUNICATIONS ENVIRONMENT

TEAM MEMBERS	David Clemente Stephen Huang Andrew Kitaka Matthew Knippen Marius Maries Vinu Mohan Michael Peterson Marek Putylo Michal Siuty Rachel Yanover
INSTRUCTOR	Alon Friedman
SPONSOR	Tellabs

TABLE OF CONTENTS

ABSTRACT

As mobile technologies are rapidly developing companies are trying to grasp the bounds of their usability to improve employee productivity. In particular, the roles and responsibilities of employees determine the type of mobile devices and applications needed to efficiently do their job. The goal of this IPRO is to develop a framework that Tellabs can use to develop mobile applications. The approach to the problem is “Any, Any, Any”: Any device (iPad, iPod touch iPhone, Droid, Blackberry, etc.}, Anytime, Anywhere.

BACKGROUND

Tellabs, Inc. provides networking infrastructure for telecommunication companies and businesses. They offer mobile, optical, and business solutions as well as global services. Tellabs' corporate headquarters resides in Naperville, Illinois. Tellabs' clients include wireline, wireless, and cable TV companies and government agencies, such as Verizon Communications, BellSouth, Vodafone, and Telecom Italia.

Tellabs wants a mobile application that provides secure access to their corporate network for all mobile devices their employees use. Tellabs main target is growth of Blackberry, Android, and iPhone platforms in their corporate environment. They wish to implement an "Any-Any-Any" policy where anyone on any personal-use mobile device can connect securely to the corporate server network, anytime.Tellabs employees currently use Blackberry, Android, and iPhone mobile devices. Tellabs wishes to devise a way to administrate them by a technology known as Afaria, which is a technology developed using Sybase Unwired platform, a software development environment that allows one application to be ported to all platforms simultaneously, by converting all the source code to each appropriate programming language.

When a prototype is approved by Tellabs, the IPRO 310 team will attempt to develop an app for Blackberry, Android, and iPhone using the Afaria software development environment to make an app that will securely interface with the Tellabs corporate server. Tellabs has informed the IPRO 310 team about certain limitations of Afaria. Tellabs will use our experiences with Afaria and user interface to create an Application that fit their needs.To do this, the IPRO 310 team will need to use the respective development kits for Afaria.

Previously developed application did not rise up to the Telllabs' expectations. The User interface was poorly designed. Although the application worked well on Blackberry platforms, the iPhone devices proved too inefficient at the time, due to the lack of multitasking, requiring many authentication steps and use of VPN. Since the executives had to exit the app and get a VPN, which they had to write down and use on the app, it was deemed too cumbersome to use.

The IPRO team will possibly come in contact with corporate and personal information. The team will also possibly have access to Telllabs' company security policy and acceptable use policy. The phones that will access the company server will be the private phones of the Tellabs employees. Putting any sort of application on phones that will be used by individuals in a private setting can put both corporate and personal data at risk. Other problems may arise if the applications are made to store log in information on each device for easy log ins. If said device is lost or stolen, large amount of corporate data is now at risk and the IPRO 310 team will be responsible for haphazardly implementing such a feature.

Lack of security in the corporate environment can lead to sensitive personal information being easily intercepted and leaked to the public. Employees and customers can sue the company for not providing effective data protection. Lack of secure communications within the company can definitively tarnish the professional image of Tellabs in the business environment.

PURPOSE AND OBJECTIVES

The purpose of IPRO 310 is to aid Tellabs in embracing current mobile technology and applications so as to increase employee productivity. The IPRO 310 team is tasked with determining employee user groups, investigating current technology to tailor to each group, and researching security solutions.

The objectives of IPRO 310 for the Spring 2011 semester were as follows:

1. Categorize roles and responsibilities of an appropriate subset of Tellabs' employees into user groups with distinctive profiles for each group.
    a. Use insights about each Tellabs group to research the mobile devices and applications that would best suit their needs depending on whether the user is consuming and/or creating data.
        1. Create guidelines for each group that depict the types of applications that are suitable for various mobile devices including smart phones, tablets, laptops, etc. such as, but not limited to, iPad, iTouch, and Droid.
        2. Investigate emerging trends in Graphical User Interface and the potential applications that could be created to empower each user group to perform more effectively
    b. Research the risks of putting confidential company data on mobile devices, provide a decision matrix of alternatives, and recommend solutions to secure the information on the different devices
        1. Identify and characterize the range of scenarios that encompass security issues in current mobile devices and those anticipated with regard to emerging technologies
        2. Draft a security policy for each device that includes where company data is stored on the mobile devices and how to secure the data if and when employees leave the company or in the case of a lost device
        3. Identify and recommend technologies needed to implement security policies
        4. Understand and characterize the usability implications of the policies being recommended

TEAM VALUES STATEMENT

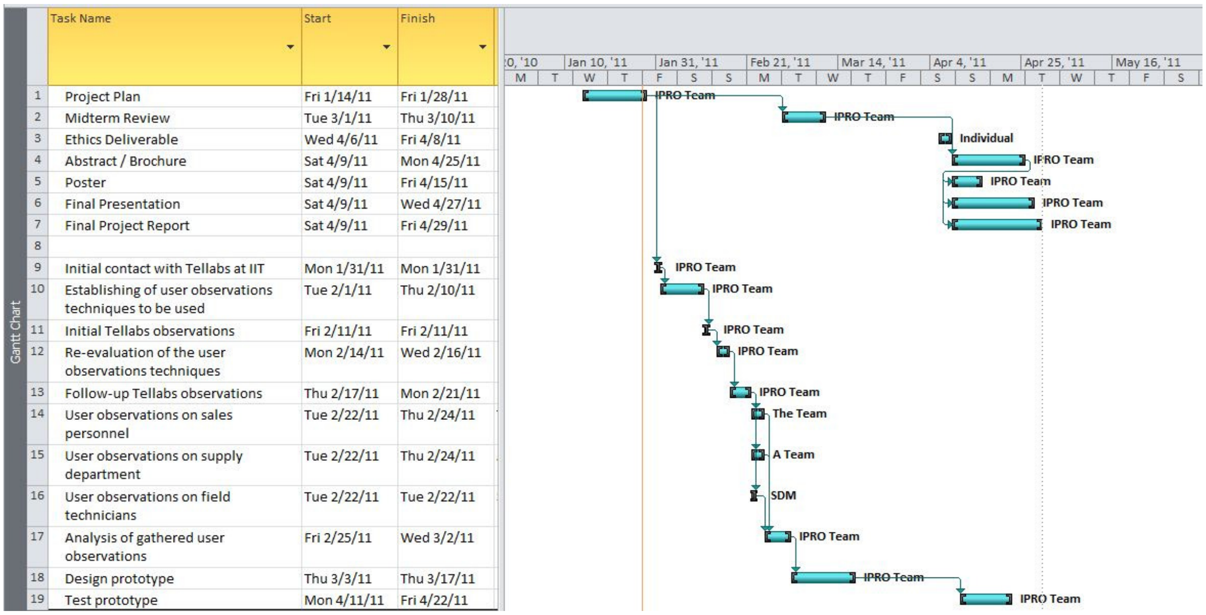
A. Desired Behaviors by IPRO 310 team members

1. Be on time for all required IPRO meetings as well as sub group meetings
2. Communicate task delays and outside time obligations in at least 3 days in advance to the event
3. Be up to date on IPRO team and customer (Tellabs) info
4. Complete respect should be given to all team members and all customer representatives
5. Respectful conflict resolution via team/instructor will take place for any conflicts among team members

B. Conflict resolution

1. The IPRO team will follow a hierarchy for managing the team
2. Subgroups will have formal leaders who communicate to the whole IPRO team and instructor
3. All peer conflicts will try to be resolved first at the student level, then the team level, and lastly with the aid of the instructor
4. IPRO 310 will not tolerate any disrespectful language or action towards any of its team members
5. During the IPRO 310 team meetings, all problems or concerns can be brought up in an open forum style

ORGANIZATION AND APPROACH



	Task Name	Start	Finish
1	Project Plan	Fri 1/14/11	Fri 1/28/11
2	Midterm Review	Tue 3/1/11	Thu 3/10/11
3	Ethics Deliverable	Wed 4/6/11	Fri 4/8/11
4	Abstract / Brochure	Sat 4/9/11	Mon 4/25/11
5	Poster	Sat 4/9/11	Fri 4/15/11
6	Final Presentation	Sat 4/9/11	Wed 4/27/11
7	Final Project Report	Sat 4/9/11	Fri 4/29/11
8			
9	Initial contact with Tellabs at IIT	Mon 1/31/11	Mon 1/31/11
10	Establishing of user observations techniques to be used	Tue 2/1/11	Thu 2/10/11
11	Initial Tellabs observations	Fri 2/11/11	Fri 2/11/11
12	Re-evaluation of the user observations techniques	Mon 2/14/11	Wed 2/16/11
13	Follow-up Tellabs observations	Thu 2/17/11	Mon 2/21/11
14	User observations on sales personnel	Tue 2/22/11	Thu 2/24/11
15	User observations on supply department	Tue 2/22/11	Thu 2/24/11
16	User observations on field technicians	Tue 2/22/11	Tue 2/22/11
17	Analysis of gathered user observations	Fri 2/25/11	Wed 3/2/11
18	Design prototype	Thu 3/3/11	Thu 3/17/11
19	Test prototype	Mon 4/11/11	Fri 4/22/11

The order in which research and activities of the project were conducted was as follows:

1. Meeting with Tellabs Contact (whole team)
    a. Met with the Tellabs point person
    (both via phone conference & face-to-face).
2. Tour of Site (whole team)
    a. Much of this project is dependent on understanding the needs of Tellabs therefore it was important that the IPRO Team tour Tellabs and meet with some of the employees of Tellabs.
3. Identify User Groups (whole team)
4. Interviews/User Observation (2 sub-teams, 2-3 people each)
    a. During this part of the project the IPRO team interviewed and shadowed the employees to find out specifics about the order of business in order to better understand their needs.
5. Data Analysis (2 sub-teams, 2-3 people each and later whole team)
    a. The IPRO team evaluated the data collected and made judgments on how it will facilitate achieving goal of the project.
6. Gathering of Information from other Companies (whole team)
    a. Used connections within other companies to know what other people are doing.
    b. The IPRO team found out about what other people with this kind of implementation are doing; we didn't want to reinvent the wheel!

7. Get any required additional information from Tellabs (whole team)
    a. The IPRO team contacted Tellabs with findings, suggestions and requisitions for any additional information that we required.
8. Proposals of Possible Solutions (sub-team, 2 people)
9. Student/Faculty Testing of Proposals (whole team)
10. Identifying Security Issues for Specified Solutions and Drafting Security Policy
    a. The IPRO team researched the security implications of mobile devices and the specific App in consideration.
11. Feedback Loop (whole team)
    a. Prototypes (Designs)
    b. Testing of Prototypes
    c. Editing of Prototypes
12. Testing, Analysis and Documentation (whole team)
    a. The IPRO team used several techniques to source the information required to identify potential solutions including interviewing employees, shadowing field technicians, creating surveys and user reviews, as well as observing users. We also used RAPID prototyping. Any progress was documented weekly and compared to the estimated progress according to the Gantt chart during the IPRO team's weekly meetings. The work was tested by the IPRO technical team. Feedback was reviewed and decisions made by the IPRO team in order to determine the course of the project.

ANALYSIS AND FINDINGS

Interviews[1]

Immediate Needs Identified

- Uploading work site pictures done through email
- Inventory on equipment with bar codes done with paper and pencil
- Technicians have to manually download important job documents onto a laptop

Other Needs

- Current VPN security authentication
- Sales approval process

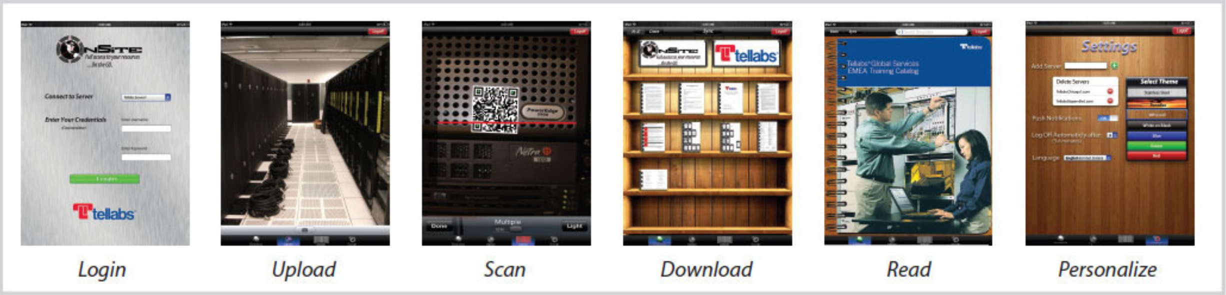
[1] Refer to Appendix E for Interview Questions and Notes

CONCLUSIONS AND RECOMMENDATIONS

Prototype

OnSite App

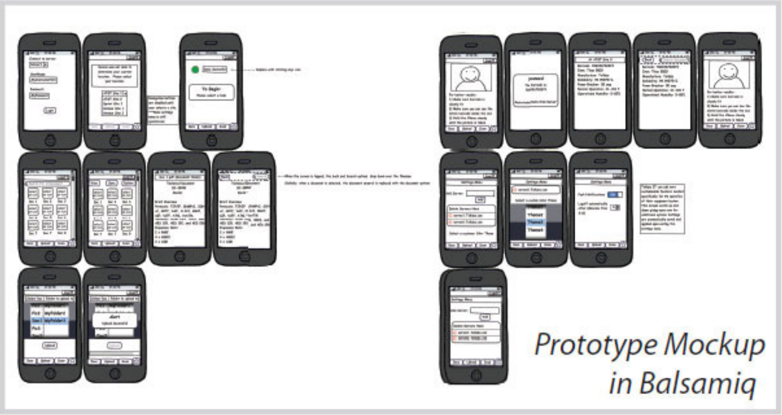
- Uploads pictures with a tap
- Scans inventory bar codes
- Keeps tech docs mobile and up to date automatically



Login *Upload* *Scan* *Download* *Read* *Personalize*

Future Work

- Implement fully functioning OnSite app on all mobile platforms
- Developing alternative security solutions
- Introduce innovations into the sales approval process



Prototype Mockup in Balsamiq

ACKNOWLEDGEMENTS

We would like to thank Ron Koestler (Tellabs Director – IT Application Development), Jean Holley (Tellabs Executive Vice President and Chief Information Officer), all of the helpful employees at Tellabs and the IPRO Office and Idea Shop for making this project both possible and successful.

APPENDICES

Appendix A: Team Information

Member Name	Strengths and Skill Set	Knowledge and Skills to Develop	Project Expectations	Contact Information
David Clemente	• Able to program in multiple CS languages • Mobile device knowledge	• Motivating others • Relying less on technology	• Making an app prototype that can be ported to all platforms	Phone: email: dclement@iit.edu
Stephen Huang	• Marketing • Sales • Entrepreneurship • Creative • Interpersonal skills	• App Development	• Create value for Tellabs through our project • Win IPRO day	Phone: email:shuang31@iit.edu
Andrew Kitaka	• IT Management • IT Security • Web Application Development	• App Development	• Get a decent App Security policy in place • Enjoy the IPRO • Build relationships with team mates • Win IPRO prize!	Phone: [redacted] email:akitaka@iit.edu
Matthew Knippen	• IPhone Developer • IPhone Security	• Understanding of how are mobile devices are being used in the business	• Develop an app.	Phone: [redacted] email:mknippen@iit.edu
Marius Maries	• Attention for detail • IT Management • Basic programming: C++, Java	• Team work • Communication • First-hand experience of a real-life project	• Satisfy Tellabs's requirements • Create strong basis for next semester	Phone: [redacted] email: mmaries@iit.edu mariuscm@gmail.com

Vinu Mohan	• Mgmt. Info Systems, Accounting, Strategy, Sales, Marketing • Business Plans • Chemistry	• App development	• Prototype app for certain group within Tellabs • Create value for Tellabs employees	Phone:[redacted] email:vmohan7@iit.edu
Michael Peterson	• IT Management • Advanced C++ and Intro Java Programming • Web Design • Networking and Infrastructure • Basic Mgmt Info	• More Mgmt skills	• Finish project and complete the IPRO for graduation	Phone:[redacted] email: mpeters5@iit.edu vet.mike@comcast.net
Marek Putylo	• Design • Leadership • Team Work • Motivation • IT Management • Communication	• Progress upon ITM • Develop major related communication skills	• To at least get the project ready for building a prototype. • Satisfy the following IPRO team	Phone:[redacted] email: marekputylo@gmail.com mputylo@iit.edu
Michal Siuty	• Organization • Information Technology and Management • Basic programming: C++	• Communications • Become more outspoken • Advanced Programming knowledge base	• Satisfy IPRO requirements	Phone:[redacted] email:msiuty@iit.edu
Rachel Yanover	• MS Office • Adobe Photoshop, Illustrator & Premiere • Writing, Organization & Communication	• Team Work • Leadership Skills	• Find and meet needs of sponsor, while creating a good basis for future ipros	Phone:[redacted] email:ryanover@iit.edu

Appendix B: Actual Budget

All materials
Materials and Supplies $950
(Describe briefly below in Justifications area.)

Travel Expenses $450
(Describe specifically below in Justifications area - re: # of trips and # of people traveling.)

Prototyping $1,100
Other Expenses $350

Justifications - Use the space below to describe expense line items above.

Materials and Supplies
Large format prints $200
Paper supply $50
Miscellaneous $75

Appendix C: Tellabs Contacts

Name	Title/Position	Role
Ron Koestler	Director – IT Application Development	Primary point of contact at Tellabs
Jean Holley	Executive Vice President & Chief Information Officer	Project supporter, participated in feedback session (project plan submission stage)
Allen Montgomery	Senior Program Manager	Interviewee
Colette Kovacs	Senior Sales Service Engineer	Interviewee
Steven Hansen	Sales Service Engineer (SSE)	Interviewee
Hari	Solutions Sales Manager	Interviewee

Appendix D: Site Visit Notes

The Following notes were taken during the team site visit to Tellabs' Naperville location on February 11th, 2011.

Michal Siuty

Training Center:

- DWDM equipment uses fiber optics to create static routes between networking devices such as routers
- This equipments is invisible to other devices
- Tellabs utilize fiber optics at speeds up to 40G and 88 laser channels.
- Usual range for the connections is about 100 miles, then signal attenuates (degrades with distance)
- 1 machine can connect up to 7 other devices in a star topology
- Their success in equipment was achieved through incorporated power balancing that allowed addition of channels without interrupting the network
- Tellabs offers technical documentation concerning the equipment
- Tellabs training focuses on installation of equipment, its operation, and acceptance testing
- Technicians usually carry a laptop or other device to read the technical documents
- Tellabs has dedicated support team that can assist technicians 24/7 with troubleshooting
- Typical install takes about 2-3 days, with larger enterprise installation it may take up to a week to install equipment
- Tellabs likes to test functionality of installed equipment before "handing keys" to the customer
- Tellabs uses SmartCore WiMAX for its mobile networking solution

  For more information, take a look at the brochure: Optical Networking Services.

General notes of in-room interview:

- Help desk uses Remedy for interfacing mobile devices
- Sybase/SAP + Afaria are used for managing Tellabs mobile devices
- They use specifically relay server to make connections between Tellabs and mobile devices

- IT creates accounts for Tellabs every user
- Users must reauthenticate when accessing different types for data
- Users get access according to their roles
- In-room presentation of <u>Workflow</u> application on iPads

Rachel Yanover

(9:06) Conference Room

- "Enrich people's lives by innovating the way the world connects."
- "Be trusted
  Innovate
  Be Accountable
  Respect
  Grow"

(9:18) 4 teams looking at mobility/capabilities

(9:21) Walking Tour

3rd Floor

- Cubicles
- Conference rooms
- Bathrooms
- Printing/copying station
- Kitchenette
- Dedicated team space (for project durations)

1st Floor

- Lobby/Atrium
- Lab
- Client conference rooms
- Coffee shop, Cafeteria/auditorium & store (run by food service company)
  - Quarterly "Townhall" meeting (global teleconference)
- Gym
  - Run by local hospital
- Training rooms

(9:36) Lab Tour

- Ken Erdelac
  - 10 yrs with Tellabs
  - Teaching & training
  - In charge of labs/maintaining lab servers
- Training environment
- Fiber Optics Relay Racks (7100s; original & nano)
  - Static route between two points (transport only- invisible to end machiens)
  - ~100 miles range

- Used in Internationally (India, South America, etc.)
- 1 machine can connect up to 7 locations
    - With 88 channels per transport span
- $500,000-$1 millions per machine
    - Pays for itself in 1-2 months
- 960 pg installation manual
    - 2-3 weeks training in lab for field employees, then reference tech. document
    - 2 months worth of training courses are available but training documents = main source of info. in the field
        - Use of mobile devices; primarily laptops
        - Issues: 24x7 call assist center @ Tellabs w/ Engineers to assist
    - No proprietary information; officially employees & customers only → not very secure information
- "8830"/"8860" Multiservice Router
- DMAX 1120 Advance Fiber Communications
    - Residential level
    - Slowly being replaced with fiber optic
- "Wi-Max" Smartcore 9160 Platform
    - New
- Echo Cancellers
    - Started company
- "5500" Digital Cross-connect
    - Put Tellabs on the map
    - 15-20 years old
    - Need for is disappearing (15-20 yrs left)
    - Recently, used at cell sites
        - Make most of existing copper cable
        - $ → avoid updating to fiber optics

(10:19)

(10:35) Meeting with IT in Conference Room

- **(10:44)** Initially looking at apps just related to SAP for mobile devices
    - But realized they have more than SAP needed to communicate to mobile devices
        - Remedy (HR), Biztalk
    - Cybase → initial choice
- **(10:51)** Went live with current system in August
- Shipping exceptions
    - Cybase platform to test as solution
    - 15-20 seconds to approve; 1 ½ minutes from laptop
- **(10:55)** "Sandboxing" w/ Cybaase
    - Security to access the app & security w/in SAP (levels of security)

- Device Recognition vs. User Recognition
- **(11:02)** App. Security
  - Levels
    - depending on types of data
    - user role/access
- **(11:10)** Example of App Currently in Use
  - Work – Flow designation/assignment by device/user
  - Account made in advance via IT department
    - Then set up on mobile device
- **(11:18)** Security Polices
  - 2: Overall & Social Media
  - Checking w/ boss about sharing more detail
  - Start with looking at Quality & Privacy of Data
  - Authentication Types in Used
    - PIN
    - Passcode
    - Certificates
    - Haven't seen need for Biometricss
  - Rejected methods? → None really outright rejected
- **(11:25) Perspectives from Field**
  - Andy G.
    - Sr. Manager in Sales Operation
    - 15-16 months with Tellabs
    - Business side of It
  - Sales World
    - Account Managers (Opportunity Stage)
      - Cultivate relationship with clients
      - Use "Sales Net" as management tool
      - "Road Warriors"
        - Rarely in office
      - **(11:33)** Major need
      - Not always able to access wireless or even landline
    - System Sales Engineers aka SSEs (Proposal Stage/Deal Stage)
      - Fill out need/meat for customers
      - "E-configure" tool
      - Desire for "offline" capacity (heavily tied to SAP)
      - Speed = key
      - Real time operation for building proposals
      - Approval system
      - "deal portal" →IGDP
  - **(11:43)** Reasons for not using? (Who/why)

        - What is convenient & easy?
    - **(11:50)** Lesson → Don't underestimate complexity of individual devices.
        - Commercial Manager
            - 10-15 globally
            - "massage" deal terms to finalize
            - Don't deal with all deals, only non-standard (~25%; ~75% go through auto system)
    - **(11:56)** Customer Master Database Issue/Challenge

Appendix E: Interview Questions and Notes

Interview Questions

1. Tech Support Guys
    - What are the responsibilities of your job?
    - What is your average day like?
    - What kind of data do you gather from the Tellabs server?
    - What are the kinds of problems technicians in the field typically call about?
    - How are problems resolved? Is there a specific application used?
    - What are the kinds of mobile devices used by technicians in the field?
    - How do field technicians connect to the Tellabs server? What do they use it for?
2. Field Technicians
    - What is the average day like for you?
    - What are the kinds of jobs you are sent out for?
    - What kinds of mobile devices do you use on a daily basis? What do you use each one for?
    - How when and why do you connect to the Tellabs servers? What kinds of data do you obtain from them?
    - Does the mobile devices you carry change depending on the type of job you are sent out to do?
    - Is there times when you need to call the Tech Support Center? What kinds of situations bring about this need?
    - Is there certain mobile devices or applications for mobile devices that you are currently required to use? Under what circumstances? Can you show us how some of these are used?
3. Sales People
    - What does your job consist of?
    - How often do you find yourself out of the office?
    - What kind of mobile devices do you use on a regular basis and how do you use them?
    - Does the mobile device you carry change depending on the clients you are meeting with?
    - Do mobile devices help you interact with clients? How?
    - Are there any problems that you currently cannot resolve while out of the office?
    - How and why do you connect to the Tellabs server? What kinds of data do you gather from it?
    - Are there certain requirements for mobile devices

Interview Notes

INFO
Allen
Senior Program Manager
JOB
Support field service groups
Creates data solutions
Works with employees to gather data
Uses a suite of tools for operation
Not really a field person, more of a support (Internal only)
Mostly in office @ home
Prepares field techs for training and development and also supports field tech directly
SOFTWARE
Sharepoint (VPN required), Infopath, Various web and excel based reports
Shareview for outside clients
FTP
EQUIPMENT
Uses PC (MS Communicator) for IM, Chatting, Video conferencing, Telecom
Blackberry for calling, txt, IM, email, communicator app
Portable scanners
All Equipment (internet included) is company provided
MOPs
Does not deal with MOPs
MOPs have to be OK'd with the customer and approved by both companies
Customer has to sign the MOP
If a SSE runs into troubleshooting a New MOP
MOPs have safe stop points where the engineer can stop and call tech support
OPINIONS
Would like more content available (more raw data storage, less file storage)
Thinks the VPN is OK
Mobile may be more cumbersome because of the office suite and program required
Some may be resistant to change
Would like an Android or blackberry device (Not a fan of the IPAD)
MISC FACTS
A lot of SSE don't have Blackberries and rely mostly on their computer
So many different systems are used because they are all rapid, quick fixes for the rapidly changing work environment and requirements
Would like to archive data instead of just moving it over to the LAN
Business requirements determine that certain documents and log files be retained for the customer for 5+ years.
Is really looking for a easy to use, consolidated solution
Tried running this program called (ISYS?), but it failed miserably because of lack or acceptance and funding

Would like to be able to see project data quickly
Does NOT want to get locked down into a large, customized system because their company constantly changes and therefore would need a very dynamic system that is easy to update/flexible, and scalable as well

INFO
Colette - Senior SSE
MBA mgt info sys
Undergrad in Political Sci
Job cycles every couple of years
DESCRIPTION
Responding through customer requests through email
Interfaces with customer
Uses computers, and blackberry, no video calling, and text messaging
Works out of the home and a lot from the road - at the customer satellite offices
EQUIPMENT
Computer Software: Outlook, word, internet, VPN, Visio
Blackberry: Email, Texts, IM
CONNECTIVITY
VPN slows the connection down for the computer
As a result, she will go through the portal than use the VPN to use econfigure
LTE card is provided to the SSE, therefore can work on everything on the go
Internet speed is limited to what the Hotel is
Does not uses the blackberry as a personal phone
Doesn't have an IPad and doesn't really know how they work
Uses customer equipment when possible (Blackberry by AT&T, etc)
She doesn't use two different blackberries
ECONFIGURATOR
eConfigure - Like a bike with a flat tire
Cumbersome and a pain
"Homegrown" - not the best coded
A change always seems to mess something else up that you wouldn't think
eConfigure is only available on PC
You can't go without eConfigure
eConfigure stores proposals
eConfigure has cusomter pricing for each part then adds to the proposal at the price point
Uses the discount
Some customers are not setup on eConfig and must use separate proposal tools
INTERACTION WITH TELLABLS
Contacts account manager via phone and email, used to be face-2-face
Video Conferencing may be a possibility?
TRAINING

Training every year (performance appraisal)
Training would be great as an app!!!!
Could never get their current system to work for mobile (via downloading training topics)

OTHER MISC APP

Implement a time management & prioritization app?
Used to have on a palm pilot
Collaborate other programs privately via email/IM

Hari

Background

10 years with Tellabs
Solutions Sales Manager
Technical Manager at Siemens (former employee)
Bachelor's in Biotechnology
Master's in Network Technology Management
20 years in the industry
-works always outside of the country (currently Kenya)
-performs presentations for customers
-mostly does trials of Tellabs products
-carries no documents in paper form
-uses the Tellabs portal
-DropBox is used
eConfigure is difficult to use
 -very complex in terms of bureaucracy not cofiguration
 -used by Sales Engineers
 -Hari does configurations all the time ON A PIECE OF PAPER

REMOTE CONNECTION TO TELLABS

-connects all the time; uses TEAMVIEWER, Windows Remote Server, VNC
-issues with acccessing the expenses site
IBM Gehrs system
it can be accessed only from Windows 7 Premium
*we need to talk to somebody who's using eConfigurator (SSE's)!!!
most used apps on phones:
Google maps
Evernote
Kindle

apps specific to job:
RF Signal Tracker - testing signal strenght FREE app NOT a Tellabs solution
2 layers of apps / tools used:
-corporate
-independent / outside of the corporation (Evernote, RF Signal Tracker)

Steve Hansen - Sales Service Engineer
Not really an average day - some day some night
Connecting Rings & International
Rings - Customer equipment that are in COs
Using fiberchannel
Mostly on the road
Working with Verizon, quest, frontier, sprint, etc.
Air port through Verizon
Computers, Blackberries - Happy With their system
He also uses Cisco Softphones for VOIP
His equipment is company Provided
Everything is electronic (paperwork)
Submissions of correspondents all kept in a file for the entire job
Would need a computer for the pure amount of work that is required. Needs a bigger screen with advanced multitasking capabilities
Personally has an iPhone and doesn't think it would work for the amount of work needed
Electronic versions of tech docs and manuals
A Tablet may be OK
Must go through VPN
WIth a PC he is able to retrieve and look at various docs from old jobs
MOP - Method of Proceedure (approvals) that are needed to be done
MOP issued by Project manager (via email) and needs alot of approvals
Must leave a copy of the MOP onsite
MOP has contact information on it for the customer
Has multiple ways of contacting the tech dept.
Content with a PC based system
Keeps personal phone seperate from Business and likes to keep it seperate
WIth a PC he is able to retrieve and look at old jobs

Appendix F: Security Research

Cellular Password Security Report
David Clemente
Michael Peterson

This paper discusses password key security on cellular devices by using an advanced method called Public-Key Cryptography. This paper will explain what public-key cryptography is, how it works, some disadvantages of it, how the distribution of the public keys work, as well as some other methods such as the advantages and disadvantages of security beacons. By now you are probably wondering: “What is public-key cryptography?”

Public-Key encryption was developed for the primary reason that flawed symmetric key algorithms. That one problem is that a computer system does not have to securely transfer the private key to the other party. While some attempts were made to make symmetric key algorithms secure, they all must send the private key to the other party. This means that a attacker can intercept the key and gain access to the encrypted data stream. This is a huge problem, and in 1976 a paper submitted to the IEEE organization outlining public-key encryption circumvented this problem. To understand how public-key encryption works, a more detailed description is needed.

The inner workings of any encryption system is very complex and requires some advanced knowledge of math and computer system operation. For the intentions of keeping this paper within 10 pages, a higher-level description will be discussed. In public-key, there are actually two types of keys. There is a public key that anyone can receive, and symmetric (or private) key that is kept secret between the two communicating computers. When transmitting, the sender uses his symmetric key to encrypt the message, then encrypts his symmetric keywith the receiver’s public key. When receiving, the receiver first decodes the incoming symmetric key by using its own symmetric key. The receiving computer then uses the decoded symmetric key to decode the data. Because of the fact that symmetric keys are based off of a primary number and are extremely long, this means that symmetric keys are almost unlimited quantity wise. Because of this, this process is very secure and allows passwords to be transmitted and verified over any network as long as the two parties receive their authentic public key from a trusted and respected source known as certificate authorities. Verisign, Comodo, and GoDaddy are just a few of the numerous, trusted Certificate Authorities (CA) on the Internet that verify these public keys. The role of the CA is to ensure that the certificate (or key) is owned by the subject that is in question and that the certificate is still valid and not expired. These CAs are independent, 3rd party companies that have a reputation, and are therefor trusted by many people who then program web browsers to trust. If a user does not want to trust a specific CA, the user can remove that specific CA from the trusted list in their web browser. However, doing this action may prevent your computer for making a secure connection if the server your computer is connecting to requires using that specific CA to get public keys. However, even though the CAs ensure that public keys are valid, public-key encryption still has its flaws.

Any downfall of any password or key in the computer world is the ability for attackers to brute-force an encryption. In recent history, for example, there have been a few vulnerabilities exploited because a key was brute-forced until an attacker broke the key. The solution to this is to make the key more complex by making it longer but, as mentioned later, a longer key has its disadvantages as well. Another downfall is the classic man-in-the-middle attack when using a compromised media such as wireless. The attacker effectively intercepts the transmission of the public keys between the sender and receiver, and substitutes in his own compromised key. At this point the attacker can decrypt and encrypt any message. This is where the certificate authority would normally catch the incorrect public key; However, if your computer has been compromised to trust a fake certificate authority then this attack can go unnoticed. Another downfall to this system is the computational power required. From the basic example given above, you can see there is a lot of tasks to perform with this encryption scheme. To keep a key more secure, it should be longer. This adds even more mathematical complexity to the scheme. Even though mobile processors are quickly evolving and becoming more powerful, so is the bandwidth capabilities of networks. Increased bandwidth requires more raw power needed to do advanced encryptions/decryptions quickly to make transfers instantaneous, just like how we humans prefer it to be. But perhaps the whole idea of public-key encryption is incorrect. While it may world well for a long distance remote connection, perhaps a more local authentication should be implemented for mobile devices.

Another potential solution for the problem of authentication on a mobile device is the concept of a proximity beacon. The idea behind a proximity beacon is that the user of the device carry around a token, some sort of device that sends out a signal. The device connecting to the network is in either one of two states: either within range or outside the range. The device will periodically check to see if it is receiving signal from the token. As long as the device is in range of the token device, the connection will remain active. Should it move out of range for any reason, the connection will immediately cease. The device connects to the token via a Personal Area Network (PAN). The most commonly used instance of a PAN is Bluetooth.
There are many advantages to this approach, primarily in terms of certain security aspects and the ease of use. It is secure in the sense that the only way to get access is to be within proximity. Essentially requiring both “keys” needed to connect to the network to be within arms reach essentially translates the problem of mobile security into a physical one, thus simplifying the process of following security procedures for many of the non tech savy end users. Additionally, since this token vouches for your identity, regardless of how many hot fix programs are used by Tellabs employees, they would not have to log in to the network. The only way for someone to intercept access would be if they were withing physical range of the Bluetooth’s piconet and were able to connect to it, which depending on their location, may be highly unlikely.

There are some significant drawbacks to using such a set up however. For one, employees now have to carry with them another device, which is another thing they have to keep track of and is another thing they can potentially lose. Additionally, the device uses Bluetooth, which obviously doesn’t power itself. Assuming there is a built in rechargeable battery, that is another device they now have to remember to charge, for if the device runs out of battery they are cut off completely and if this was the only way they had to access the server, they have no way to authenticate. Perhaps the greatest flaw of all with this approach is that the token connects to the device via Bluetooth. Bluetooth has major security flaws that to this date have yet to be fixed. Some of the more dangerous exploits of the Bluetooth connection allow a hacker to take partial or complete control of a device (depends on the device in question). More likely to occur, is the situation where an employee tries to access the server in a public location (a coffee shop perhaps?) and someone else will be able to use their token to authenticate into the Tellabs server. Possibly this can be avoided by tying the authentication to both the token and specific devices for that token, but this may be hard to implement and enforce. However, aslong as one keeps track of their devices, keeps them properly charged and is able to limit how many people around them are privy to the existence of their token, the chances of the drawbacks actually becoming a problem are significantly lower, and in such a case the benefits of this set up while shine through.

From the thoughts and technologies such as beacons and some ways that they can help or be hindered by existing technology that already has flaws, to the advantages and disadvantages of the older public-key encryption algorithms security is always changing to meet the demand. In the end, it is not just one thing that constitutes a secure system. In the real world it takes multiple systems and schemes to make a system secure. Because of these reasons, network security personnel are becoming a important asset. With the ever increasing prominence of smart phones in our everyday lives, it becomes increasingly important that the data that comes to and from, and is stored on our phones is secure. This becomes especially important in a corporate environment such as Tellabs ,where one security flaw could be fatal. Thus the demand for secure and easy to use security protocols is huge, and only getting larger.

Bibliography

Certificate Authority. (2011, Mar 27). Retrieved Apr 01, 2011, from Wikipedia: http://en.wikipedia.org/wiki/Certificate_authority

Jansen, W., Gavrila, S., & Korolev, V. (2005). *Proximity Beacons and Mobile Device Authentication: An Overview and Implementation.*

Public-key cryptography. (2011, Mar 21). Retrieved Apr 01, 2011, from Wikipedia: http://en.wikipedia.org/wiki/Public-key_cryptography#Distribution_of_a_new_key

Rhodes, C. *Bluetooth Security.*

Rothman, M. (1999, May 17). *Public-key encryption for dummies*. Retrieved Apr 01, 2011, from WorldFusion: http://www.networkworld.com/news/64452_05-17-1999.html

Symmetric-key algorithm. (2011, Mar 28). Retrieved Apr 01, 2011, from Wikipedia: http://en.wikipedia.org/wiki/Symmetric_key_algorithms

Tyson, J. (2001, Apr 06). *How Encryption Works*. Retrieved Apr 01, 2011, from HowStuffWorks: http://computer.howstuffworks.com/encryption3.htm

Mobile Authentication
Matthew Knippen

Every company has a need to prove who is accessing there network and making sure that it is secure. Over eighty percent of the Fortune 100 companies are using iPads in their business now, so how are they overcoming that problem?

The ideal way for any authentication is by combining something that you have with something that you know. By having both of these characteristics, it would be very difficult for someone to fake being you. The simplest way for a company to make sure that a person is using their own phone is requiring a password. By also using advanced technologies to verify that the person is using their own phone, we are combining something they have (their phone) with something they know (the password). Using this rather simple implementation, any company can be very secure with very little effort.

However, many top companies are not even using this much security in their networks. Having worked for both IBM, and Apple Computer, as well as designing iPhone and iPad applications that require security measures for a corporation. Most applications simply require an advanced 8-digit password. This is used in the Apple Store when an employee chooses to buy a product. The employee must enter a password to complete the sale. At IBM a password must be entered to read e-mail, surf the internal web, or to access other VPN. Using a password that the average person could not easily guess is key.

Alex Bratton, the CEO of Lextech Global Services, stated that if you are using VPN on a service, that you need a mobile app created for you. He stated many reasons, but the main reason is that VPN is a slow and clunky tool that old and outdated. Companies are still using this even though there are many better solutions available. SSL encryption is an advanced way to make sure that no other person can be stealing the data from one device to another. This means that when an iPhone connects to the company’s server, no one else can intercept the data, making this very secure. SSL is a very advanced encryption method, but luckily it is easily implemented by any iPhone developer. SSL has now become a cheap, easy and secure way to keep transferring data secure.

As you can see, using SSL with a password authentication is the ideal way to verify who it is that we are talking to. If the company is really adamant about additional security, we can choose to verify the phone matches up to the user. This is an additional security measure, but it is good to have because it does not interfere with the user.

Securing Mobile Devices and Information Resources
Andrew KITAKA

In talking about information security in mobile devices the key checkpoints of the data are: the confidentiality of the data, its integrity, and its availability. These are the main standards by which information security is measured. Data must be accessed by the right people for whom it is intended; data must also remain as original as it was sent from one user to the other, as well as be accessible when it is needed. In order to secure information resources we must be able to secure the devices used to transmit this data.

The first step of mobile device security is the device's physical security; knowing at all times where the device is the most important part of securing the device. Once the device is physically accessed then the risk of accessing the content also increases.

There are however other ways that Mobile devices like the iPad have ensured the integrity and confidentiality of data. The first line of defense for the mobile devices is passcode authentication; numerous devices have passwords, passcodes, or patterns by which they identify the right user. Using these user specific password data contained on the device is sure to be confidential in that it is only accessed after the correct passcode is entered.

Another way information resources on mobile devices can be secured is by encryption; many of the devices on the market support specific applications that ensure that data transmitted through them is encrypted. Strong encryption patterns are use to secure information as it is transmitted over the internet; other devices such as the iPad even have hardware encryption for the data that is resident on the device. This improves the security of the information resources on the mobile device.

The iPad for example has enabled, by default, 256-bit AES encoding hardware-based encryption to protect all data on the device. Along with this, the iPad can be set to locally wipe the data on contained on it after a set number of failed passcode authentications; also with the help of remote administration tools you can remotely wipe the data on the device.

Another important option of securing information resources on mobile devices is the use of secure networking protocols like VPNs to access sensitive information, in this case, the device access the sensitive information of a secured connection across the internet. Data and information resources that are deemed sensitive are not resident on the device but it is only used to access the data.

All the above options work together to ensure the security of information resources on mobile devices. It is however important to note that security cannot be certified as total; information resources can never be hundred percent secure; it would be a myth because it only takes one leak to disprove such an assertion. Therefore the goal of information security professionals is to provide as much security as possible for a device at any given time, and to monitor, working proactively and reactively to ensure that any security vulnerabilities are addressed and any security breaches are quelled.

References

http://images.apple.com/ipad/business/pdf/iPad_Security_Overview.pdf

Security Trends in Mobile Devices
Michal Siuty
Marek Putylo

Over the years, we have seen the rise of mobile devices. Thanks to increase in functionality and advancements in computing technologies, mobile devices are rapidly becoming PC and laptop replacements. They play a large role in market share and due to that change, mobile implementation in business and enterprise across the globe has risen drastically. This means “that private information of the user - such as social media interaction, private telephone calls, text messaging, web browsing - becomes intertwined with corporate information such as emails, documents (receiving, amending and sending) and calls”, as Marc Smeets states in his article Security Trends in Mobile Devices: What do businesses need to know?. New concerns of mobile devices fuel the emergence of new security trends and enhancements for both private and corporate data protection.

Mobile device trends include:

- Remote management of mobile devices:
    - Mobile devices can be controlled remotely, device can be locked or wiped clean of data
    - For example, Google has developed remote malware removal feature for Android devices
- Implementation of biometrics security
    - Implementation of biometrics is easy because commonly included feature of a mobile device is a high-megapixel camera capable of facial recognition and a microphone
    - Biometrics security is based more on application software rather than hardware and could be more easily developed
- Desktop/laptop replacement
    - Huge variety of application can be run and accessed on the mobile device
    - Advancements in technology enables to run more complex processes and allow multitasking
    - 3G/4G and Wi-Fi networks allow user to surf the web as if he/she were on their home computer
- Increased consumerization
    - “Bring your own device to work” for replacing company provided mobile devices with one’s own
    - Private and corporate use of the same device
    - Jailbreaking the device or installing pirated software may cause more exploits but allows more capabilities of the device

Due to the higher use of mobile devices, they are more often becoming target of a malicious attack. Because of small size, mobile device is susceptible to theft or misplacement. Unintentional loss could result in leak of sensitive personal and/or corporate data. Another common security risk associated with mobile devices is application exploits and spreading malware. Mobile devices were originally targeted at individual users and often lacked appropriate security measures that would satisfy corporate standards. Lack of properly encrypted communication can result in data sent being intercepted and hurting both unaware user and the business.

Mobile Device authentication (look into sources for more details):

- Microsoft SharePoint – access through browser or client application
  - VPN - server access over SSL
  - Mobile proxy server – use servers like MS System Center Mobile Device Center and Blackberry Enterprise server to access corporate data
  - Direct Internet access – basic authentication, but can be combined to support SLL and other security standards
- ARM TrustZone – hardware implementation to securing connections
  - Can capture data inputted from the keypad and send it securely over and encrypted connection
  - Can thwart spreading of malicious software
- Usage of QR codes
  - QR codes can be used to create accounts without the need to generate random username or password
  - Password can be very long and complex without need to memorize them
  - Quicker login, encryption mechanisms available, anti-phishing solution
  - Drawback – can be susceptible to MITM, user cannot access website with other device, attacker may use phone to impersonate the user
- Soft Tokens
  - Enhance user convenience and allow quick distribution
  - Eliminate need to carry hardware device
  - Compatible with OATH HOTP open standard authentication

Sources

Trends:
http://www.thirdfactor.com/2011/03/23/biometric-trends-will-emerging-modalities-and-mobile-applications-bring-mass-adoption
http://www.datalossbarometer.com/14718.htm
http://www.processor.com/editorial/article.asp?article=articles%2Fp3301%2F21p01%2F21p01.asp
http://techaxcess.com/2011/03/mobile-browsers-big-security-hole-in-a-small-package/
http://www.betanews.com/joewilcox/article/Google-removes-Android-malware-so-you-dont-have-to/1299469153

Authentication:
http://technet.microsoft.com/en-us/library/gg610510.aspx
http://www.arm.com/products/processors/technologies/trustzone.php

http://corp.galois.com/blog/2011/1/5/quick-authentication-using-mobile-devices-and-qr-codes.html
http://www.actividentity.com/products/authenticationdevices/SoftTokens/