Agenda

• Security Overview
• Setting the Stage
• Some Good News – Voice and Video
• Controlling Newer Systems
• Educate Users
• The Future
Security Overview
Security Levels

Complexity $$
Manpower
Overhead
Equipment

Complex
Intermediate
Easy
Encryption

• Pros:
  Secures the system in such a way that user data is protected in transport
  internal
  Data at rest and data in motion encryption is the goal in high security
  environments
  Can terminate it on an SSL accelerator (ACE Module as an example) so you
  can still inspect that traffic

• Cons:
  Makes the network blind to the traffic flows if terminated on the application
  Can add additional overhead to the application itself if SSL acceleration is not
  used
  The best way to attack the system is through the encryption
  Overall complexity of the deployment of any application increases
  If used for external sites applying enterprise security is much harder
Setting the Stage
Main Issue.....

• Users are driving enterprise communications
  The device
  The type of communications
  Expected ease of use that they have at home
  Freedom to express anything happening to them

• If the users do not like the IT solution, they use what they want

• Have very little care about security
  If they are not concerned about their security, are they concerned about yours?

• Will be based in the cloud, with non commercial software and that usually less secure then eternal applications
Systems for User Communications

• Even in the cloud, users have a choice
• This is the short list – worldwide there are many others
User Communications Software

• Just some examples of what user have to choose from

• Voice, video, IM, it could be a very long list
User Remote Storage

- Storage of critical docs could end up in these areas

Home SAN

- Iomega
- Google Docs & Spreadsheets
- Dropbox
- Microsoft Office 365
Communications Devices

Tablet and Phone From Cisco

Tablet and Phone With Android

Smart Phone From Apple

Phone From Motorola

© 2010 Cisco and/or its affiliates. All rights reserved.
Classic Examples

• An employee at a company see’s something funny at a company party
  They take a picture with their phone
  Upload it to Facebook
  Tag it with the persons name
  Facial recognition finds all photos of that person on Facebook

• An employee wants to capture something on a whiteboard
  Takes a picture with their phone (Android, Blackberry, iPhone)
  Uploads that picture to Dropbox (or similar system)
  Goes back to their desk and downloads it to their desktop
  What was the information and should it have left the building?
Interesting User Behavior

- Users will post information to unsecure environments that they would not send in corporate email
- Users are bleeding their personal behavior into the corporate environment
  Their lack of security for themselves can affect a corporation
  What is acceptable at home is not always acceptable at work
  Example:
    Photos from vacation of their partner in beach clothes might not be acceptable in some countries
    Should those photos be allowed at work?
    If they are not, will they just send the link around in email anyway?
Some Good News
Enterprise Voice and Video (IP)

- When VoIP systems first came out, it was the wild west just like with new communications systems today
- The wild west days are long over, enterprise voice/video can be controlled and secured
- The security tools and monitoring caught up with this new communications tools
  - Firewalls
  - Recording – both encrypted and non-encrypted
  - Segmentation
  - Leaving the enterprise into the service provider space
  - Etc.
What we did for Voice and Video
Rank Your Data

- Don’t make security an end to itself
- Rank the data by your business requirements
- Evaluate whether your existing security policy is sufficient
- I can not tell you how much security you need
- I can help you determine what is acceptable to you and your management
Security Deployments - Voice
All the Possibilities
Highest Security Questions asked by Customers About VVoIP

• Eavesdropping
  Listening or recording data without approval

• Denial of Service (DoS) or Distributed Denial of Service (DDoS)
  Flood bandwidth or resources of a targeted system

• Impersonation
  Attempt to be something or someone that you are not

• UC applications security
  Application layer security

• Soft client
  All non-hard phones, could be voice, video or instant messaging (IM)

• Toll fraud
  Making calls that the users is not approved to do, usually long distance calls
Voice and Video Traffic Flows
Peer to Peer Communication

Cisco Unified Communications Manager

Gateway To the PSTN

TLS Signaling

TLS Is Client Server

SRTP Is Peer to Peer
Firewalls and Real Time Protocol (RTP) (problems overcome)

- Signaling makes a firewall work
  As long as the firewall understands the signaling, RTP will function correctly

- If you upgrade a voice application server the firewall might be affected

- As we add new media to the solution it might not work through the firewall day one

- A constant battle to keep up with the changes

- Check the software compatibility list from system test on
Firewalls and RTP

• Move the firewall a bit
  Now the firewall does not see the signaling
  Media will not flow through the firewall
  Calls will not complete
  Peer to peer vs. client server

• Can make VoIP designs hard with firewalls

• Have to open up the UDP port range for RTP to make this work (ACL)

• Most firewall deployments are centralized to make sure that the signaling runs through the firewall
Remote Phones

- All traffic from the phone is in the VPN
- The phone only does:
  - Traffic to and from itself
  - Does not do any other traffic
  - The PC plugged in will have to do its own VPN
- Some companies are using
- VPN for hard phones
  - If you have lost physical control of the hard phone, can use the VPN
  - CUCM 8.x
Toll Fraud: CUCM

• Traditional dial plan configs as on all call processing devices
• Call forwarding, remote call forwarding, and trunk-to-trunk transfers
• Partitions and calling search spaces limit what parts of the dial plan certain phones have access to
• Dial plan filters control access to exploitive phone numbers
• Ad hoc conference calls can optionally be dropped when the originator hangs up
• Forced authentication codes or client matter codes prevent unauthorized calls and provide a mechanism for billing and tracking
Unified Communications Policy

• You need a security policy for voice/video/IM style of data

• Look at the overall system
  What does it look like compared to what applications are already on your network

• Have a way to respond if something does happen
  How will the issue be addressed?
  What are the repercussions to the attacker?

• Make sure that management knows the defined risks
  If they know the risks going in, better decisions can be made
  If security does need to increase—this will help define expenditures
Controlling Newer Systems
Social Networking – Good vs. Evil

• The Good (and kind of amazing)
  Knowledge travels faster and farther than ever before
  Groups form to solve problems on their own
  Creates a community at work that is new
  Motivates people to create content or share information on their own
  Many forms of communications right from the browser

• The Bad
  Knowledge travels faster and farther than ever before
  Tools are not in place to control and secure this data
  Users can put information external that should never leave the building
  Today we have to rely on the users to be smart about this information
Examples of Cisco Quad
Examples of Cisco Quad

- IM
- Voice
- Video soon
- Meetings
- All in the browser
Can It Be Stopped?

• The short answer is no

• Like IM before this will become mainstream communications

• On the way to mainstream systems have to be created to control
  The content created
  Storing of that content
  Who can post content
  Who can see content
  Security of the content
    What level
    Who created

• Do internal - Legality and compliance is under your control

• Do it internal of the users are going to do it without you – and do it external
Can It Be Banned?

• Maybe

• Some people in this room might have the power to do so

• Some environments should never have social networking software

• The users might not have –
  Cell phones at work with cameras
  USB drives they can carry out
  Cameras at work
  Any tool that can be used to push data to the web

• URL Filtering – hard to keep up

• In most work areas this is not realistic to expect this to happen
How Can it be controlled Internally?

- There are several models of controlling the flow of information
- Have the users police the content
  Like they are used to on the web – Wikipedia
- Report bad content to admins of the system
- Have content moderators that respond to issues
- Have tools to monitor the content that is created
- URL Filtering for external systems
  Smart users can work around this issue
Educate Users
Train and Trust Users

• Define to the user what is appropriate behavior in the system
• Let the users help define what content is good work your work environment
• Give the users the ability to report bad content within your systems
Use Policy – Security Policy

- Have a security policy to let users know what will happen
- Most people do not want to lose their job – they will follow it
- If they don’t want to lose their job – they really don’t want to go to jail
- Define what minor and major issues are and what the punishment will be
The Future
All Your Eggs in One Basket

• Enterprise social networking software is coming (or it might already be here in your network)

• As shown earlier, all content and communication can be within that system

• Plan for this technology adoption, do not just let it happen to you

• User control and content control is key
  
  Give the user a system that keeps them from using external ones
  
  Train the users about correct behavior
  
  Have a policy that defines what could happen to the user
  
  Give the user the control appropriate for the environment they are working in
Thank you.