Designing an Enterprise GIS Security Strategy

Learn about Esri’s security strategy and gain an understanding of the principles, patterns, and mechanisms involved in designing your own enterprise GIS security strategy. This session covers the principles Esri employs to support successful deployment and operation of secure GIS solutions, security patterns identified by Esri that you can apply to your situation, and security mechanisms available to you within Esri software. The session invites feedback on current security issues and concerns.

http://video.esri.com/watch/94/designing-an-enterprise-gis-security-strategy

---

Video Transcription

00:01 So today we'll be talking about designing an enterprise GIS security strategy.

00:06 We'll have a brief introduction, find out a little bit about you guys, too, myself...

00:11 ...talk about Esri security strategy we're working on...

00:15 ...various deployment patterns we've been working on for the last couple of years...

00:19 jumping into various IT security trends out there...

00:23 ...and then talking about mechanisms that you can deploy across our various enterprise products.

00:29 Then drilling into more product-specific options, be it for ArcGIS Server, desktop solutions...

00:35 ...mobile solutions, and cloud computing.

00:38 So that last one, cloud computing, I, I've had to spend a good amount of time over the last couple of months ramping up in that area.

00:45 That's been a, quite an adventure. So, and then the recap and summary.

00:52 So part of this session is also to get feedback from our customers, too, what key things are of interest and of concern to you.

01:00 So that will be going on today too. So myself, I'm an enterprise architect within Esri's Professional Services Division.

01:08 I'm also a FISMA certified and accred...accreditation application security officer; the federal agencies refer to that as an ASO...

01:17 ...application security officer, A-S-O, hey!

01:21 When you think of security, what do you think of? Okay, there we go!

01:25 So a certified information system security professional, and that's enough about me.

01:31 So the question I have for you guys...this is a simple one... Are you happy with your current security?

01:37 If you are, please raise your hand.

01:43 Hey, I got one hand, I'm impr...oh, two, okay. Okay, so why do I ask this question?

01:51 So, in 2009, Department of Energy National Labs put together a nice little list of security maxims...

01:57 ...so...sayings, adages, and so forth.

02:00 So they're true about 80 to 90 percent of the time; I think you'll like this one.

02:05 The "So we're in agreement" maxim, they called it.

02:10 So if you're happy with your security, so are the bad guys. So...

02:15 ...so now a good point in your defense is that, hey, that 80 percent...

02:20 ...an 80 to 90 percent means that 10 to 20 percent of the two of you actually do have good security.

02:30 So, we'll move on here.

02:32 So, what does a secure GIS mean to our audience here in this room?

02:38 Is it simply a matter of, okay, I noticed that somebody said I have clear text passwords, so I needed to turn on HTTPS...

02:47 ...or utilize this thing called SSL, put that in place, I'm good; there's this encryption thing going on.

02:53 Or is it as simple as, I go to ArcGIS Server and I push a button to turn on this thing that actually does say, Turn on security...yes.

03:02 Does that take care of the security for your enterprise?

03:06 This session's more about not just particular implementation options and how to do those options but more about...

03:13 ...the options available across your enterprise and how our products fit into that.

03:17 So integration with your various directory services, be it LDAP or a Microsoft Active Directory structure...

03:24 ...how we fit in with various standards, certifications, and regulations out there.

03:30 So, FDCC...this is something we've started doing over the last couple of years...

03:34 Federal Desktop Certified Configuration.

03:37 All federal groups have to lock down their solutions to a particular hardened configuration for desktops.

03:44 And products have to fit into that. So we've begun a self-certification process aligning with that.

03:50 FISMA is federal groups for not just desktop but information system security in general.

03:57 The various user interfaces out there...so we have quite a few now, or APIs, so we have...the ADF.

04:04 You have Silverlight, Adobe, Flex, JavaScript, and various rich clients.

04:09 So why would this have an effect? So let's take Adobe Flex.

04:13 So what is the most...a common...attack surface, on a lot of Web applications right now?

04:20 It actually is through that Flash-based plug-in on browsers. So it's something to be aware of...

04:26 ...that that can affect your enterprise implementation...and how you can go about updating those in an effective ma[nn]er.

04:34 So there's also application versus security products. What do I mean by this?

04:38 So this is how much security functionality Esri offers out of the box with our token service...

04:45 ...versus when you need to start looking at various third-party solutions on top of our products.

04:52 So the key here is don't focus on trying to implement just a single security silver bullet.

04:59 As far as our security strategy, so there's a couple reinforcing trends to our security strategy.

05:05 One is about our products.

05:07 So previously we've moved from discrete products, operating individually, to more of a uniform enterprise solution.

05:15 Along with that, our security models changed a little bit in that we really didn't have much in the way of a security model...

05:21 ...with our early-on products. We relied on our customers to implement third-party mechanisms on top of ours.

05:28 Now we do have some embedded security functionality.

05:31 And I'll even talk about some new functionality that may be getting integrated with our product over the next year or two.

05:39 So IT trends...so, moving from isolated systems to more integrated enterprise solutions...

05:45 ...where you have discretionary access amongst them.

05:50 Then for our...as far as the actual components of the security strategy, we have secure GIS products...

05:55 ...which, where we incorporate security industry best practices that are trusted...

05:59 that provide trusted geospatial services across the globe...

06:03 ...that meet the needs of individual users and entire organizations.

06:08 So we also provide some solution guidance via...Resource Center is one component.

06:15 It's a Web site we put together over the last year and a half or so, and I'm trying to pull it up here live...there we go.

06:23 And so in the Resource Center...was...the overall Resource Center was updated at the...

06:29 ...in this list here, you have enterprise GIS. So it's sort of tucked away.

06:34 But it has quite a bit of content in it once you get into it.

06:38 So enterprise GIS area is about architecture security and performance.

06:42 One thing we added over the last month is that your information and links for these various pages are all version, now, specific.

06:51 So I switched to 9.3...my now helpful resources are about 9.3.

06:56 All of the pages I drill into here are about 9.3 as opposed to 10.

07:01 So basically, you split down two different paths, but the sites look very similar.

07:07 So in this site, we have strategy options, which we'll be talking about today...

07:14 ...security mechanisms deployed across the enterprise...

07:17 ...and application-specific functions. So you can drill down into...well, I'm interested in...

07:23 ...what are some of my authorization options across the enterprise with Esri products?

07:28 And then I see a link in here for, you know..

07:30 ...hey, I would like to see a sample of this idea of hiding some objects within the application.

07:37 Now notice it jumped into 9.3 help, so in the 10.0 site, it'll jump directly into the 10 site.

07:46 We also will be making slightly different...we'll be updating the architecture representations specifically for 10 versus 9.3...

07:55 ...so that there's not as much of this question of, well, so I went to the Resource Center, you know...

08:00 ...the Enterprise GIS Resource Center...I wasn't quite sure it was applicab...applicable to me; you know, I have 9.3...

08:07 ...but there's this stuff out there...was it 10? Which is it?

08:10 So that's why we went with the version strategy.

08:14 So another key area is the Implementation Gallery. So this is where we provide helpful documents, test results for performance testing...

08:25 ...some security hardening guidance of systems.

08:29 And here specifically is a security guide on .NET Active Directory membership providers.

08:36 So it's a...called a custom provider, and we'll talk a little bit about that more soon.

08:44 So as far as our security strategy, it's based on a couple of key core security principles.

08:50 So you have the CIA security triad, consisting of confidentiality, integrity, and availability.

08:56 Now, one thing that 's very common for GIS users is they go, Well, you know what, my end result is primarily public data...

09:04 ...so why is it that my security guy is bashing me over the head to lock things all down on my system...

09:10 ...when the end result is I want to give this information to the public?

09:14 Well so, that one of giving information to the public; that's addressing...we're talking about confidentiality.

09:20 But integrity...so if somebody was to take your public Web site...let's say it's parcel information, manipulate a parcel...

09:29 ...because now there's Web editing...and maybe adjust a parcel to their advantage, and then they present that to another party...

09:37 ...using your Web site, that you said, Hey, I'm serving public information, somebody manipulated it.

09:43 You have an integrity information issue.

09:46 There's also availability...its relationship to security, you have these denial-of-service attacks that are not that uncommon, actually...

09:54 ...where somebody can come down...come out, just hit your site real hard, and take it out at the knees.

09:59 So what if your site was providing emergency operations information to the public?

10:05 It didn't matter if, you know, as far as somebody hacking; that you weren't too concerned about that.

10:11 But you were concerned about making sure those people have that information 24/7.

10:17 So defense in depth. This is, ideally, you have a whole bunch of layers of security across your organization, at different levels.

10:25 So this representation here, I have data and assets at the core protected by physical controls...

10:31 ...be it how you lock down your data center, your doors, and...is your server actually locked up in a rack...versus policy controls of....

10:41 ...how often you change your passwords and other components like that.

10:47 Our primary focus here today will be about the technical controls or mechanisms that you can deploy across the enterprise...

10:54 ...because there's more of a direct correlation with technical controls and our software.

11:00 So there's authentication, authorization, filtering mechanisms, encryption, and logging.

11:05 We'll talk about all those more soon.

11:11 So our security implementation patterns are based on best practice guidance that we've accumulated over time.

11:17 They'll leverage also the National Institute of Standards and Technology guidelines...

11:22 ...for a low-, medium-, and high-risk type of environment.

11:25 We also...so the key thing of this is, the first thing you need to do is understand where you fit in this.

11:32 So, am I a basic or standard type of need or advanced type of need? And how do I go about doing that?

11:38 So I'll talk about that relatively quickly.

11:41 So...choosing the right pattern...you can go the formal approach; all of our federal customers have to do it.

11:47 They don't really have any choice.

11:50 So there's this publication out there...860.

11:53 Some actual large corporations follow this same type of guidance.

11:57 There's also, we've also created a more informal process to give you a better feel...

12:03 ...rule-of-thumb type of direction, for going the right path.

12:07 So for a basic security type of environment risk...there's no sensitive data; it's public information.

12:14 This is where you can start, you can have, pretty much, your architectural tiers combined into one...

12:18 ...be it your Web, app, data, information.

12:21 In a standard environment, you need to start breaking out these components from each other, because there's a...

12:27 ...where there's more moderate consequences for data loss or integrity.

12:31 And there's also a potential need for federated services...

12:34 ...so this is where you have potential more integration with other businesses...

12:38 ...and communicating with those other businesses in a secure fashion.

12:42 And last but not least is advanced security needs. I have sensitive datasets.

12:46 All the components are now needing to be redundant to ensure that availability component.

12:51 It's also where you need to think about utilizing more and more third-party enterprise security components...

12:56 ...on top of our basic security functions.

13:01 So a basic security environment. What is it? What are some attributes of it?

13:05 Well, in this case, I have a Web application with both anonymous users and authenticated users.

13:12 I'm also utilizing some ArcGIS Online basemaps.

13:16 This is a public cloud reference down at the bottom; it could be Google's; it could be Microsoft just as well.

13:24 So you're use...but one thing to note also is the API, by default with ArcGIS Server, is coming from ArcGIS Online.

13:32 So it's just a dependency you have that you need to be aware of.

13:36 So you can secure the services with a token service that's adequate for this type of model.

13:41 And you want to separate your internal systems from Internet access with a DMZ, very common.

13:48 And then a re...reverse proxy, to avoid DCOM calls across the firewalls.

13:55 So I haven't made nice little diagrams yet for the standard and advanced environments.

14:00 I have more of a list of common attributes.

14:04 It's quite an adventure to come up with a diagram for these environments and not get critiqued to death.

14:10 So I figure I'd start with the attributes and then work up to the diagram.

14:14 So, for the standard environment, you also want to just think about a component called a Web application firewall...

14:21 ...in addition to your reverse proxy, or in place of a reverse proxy. I'll talk about those more soon.

14:28 You also want to utilize dynamic based tokens.

14:30 You don't want to use these static things, just make them long-lived for, you know...

14:34 ...one year and hope that nobody compromises that over time.

14:38 You want to separate the tiers out, which we've talked about a little bit before, the Web database.

14:43 And even management systems, especially even on the...the supporting network infrastructure.

14:48 So there's this idea of a flat network where all my systems are...have access to each other, or you start segmenting it with VLANs.

14:57 Ideally, you start doing that in the standard environment.

15:01 There's also multifactor authentication utilized for external users of the solution.

15:06 And you want to separate management traffic connections and have redundant components, local copies...

15:12 ...for your datasets for high availability.

15:16 This is where you want to also start thinking about those APIs I mentioned that came from ArcGIS Online [dot]...by default...

15:22 ...or ArcGIS.com, by default.

15:26 You want to start deploying those locally, on your local server.

15:30 Do you have an SLA with ArcGIS Online, or an external cloud provider...

15:35 ...to ensure that those are going to really remain available for you?

15:39 So that's the reason you want to have those locally in this type of environment, to ensure that you're meeting your SLA requirements internally.

15:47 So you also want to ideally utilize what are called intrusion detection and prevention systems...

15:52 ...lock down various ports and protocols and services.

15:55 There's a nice hardening...system hardening guidance white paper that we've put together.

16:01 And we'll be updating that later on this year for 10 and Windows 2008.

16:06 You also want to standardize your system images, be it virtual images, AMIs from Amazon, or within your own enter...

16:15 ...en...organization or enterprise, be it with Microsoft solutions.

16:21 So you also might want to utilize host-based firewalls on your individual servers.

16:26 And last but not least, in this type of environment, browser plug-ins start kicking in, so...

16:30 ...be it for Silverlight or Flex, and so forth.

16:36 For the advanced environment, you have minimal reliance on external data and systems.

16:44 So starting to remove those external dependencies as much as possible.

16:48 You want to separate your datasets, be it public employees, a...a subset of those employees, and so forth.

16:56 You might want to start getting into labeling your datasets, as it's called.

17:01 There's also some options called transparent data encryption that can be utilized against a database system.

17:07 And utilizing third-party security mechanisms to secure your Web services traffic.

17:13 So there's quite a few of those.

17:16 There's public key infrastructure certificates for client-side validation.

17:21 When you have local users accessing the solution, you ideally would be using what's called multifactor authentication.

17:28 Something you are, something you have, something you remember...there's multiple factors for accessing a system.

17:36 And so remote users access via hardware token multifactor authentication.

17:45 And you have network connections that are redundant with ideally .NET IPSec traffic between those servers.

17:52 Utilize SSL transport layer security between your clients and servers, for both Web and rich clients, so desktop solutions.

18:01 And then there's also this idea of network access control.

18:04 So that's a...the idea is basically, hey, if I had somebody with a laptop that comes into my organization, they plug in the connection...

18:13 ...the systems check to see if your laptop even has the right security patches on it before it can become a part of your network.

18:21 So it's a[n] interesting concept and used by some of our customers.

18:26 So jumping into some security trends here.

18:30 So I did a quick Google trends here in the lower left...of the term cyber security, and how it's changed over time.

18:38 So starting off in the '90s...it started off, brief discussion...but for some reason, it peaked up in 2003, 2004.

18:47 You had Code Red, you had Melissa...do you remember, anybody get that "I love you" e-mail from good ol' Melissa?

18:55 So there were some interesting ones out there. This is a time when there was a discovery process that, hey, we're getting on the Internet...

19:03 ...we're having a whole bunch of you people use things...boy, we really need to lock things down...Microsoft.

19:08 This is Microsoft's discovery period, ha!

19:12 But as you can see...2005, 2006, 2007...there was sort of like this tapering off interest...and...

19:21 ...but all of a sudden, in 2008, 2009, there's increased attention, and we'll talk a little bit about that soon.

19:28 So this guy is an interesting guy, one of the early hackers. His code name, we'll call him Captain Crunch...because what did he do?

19:39 He basically took the plastic whistle out of a Captain Crunch cereal box, blew it into his phone...

19:47 ...and discovered that he could get free access to AT&T's whole network.

19:51 So, one of the first early hacker attempts by an individual.

19:57 So where are we at, getting closer today? What are the types of attacks?

20:02 Well, we have people trying to get the attention of the president, Hey, candidates, you know what?

20:08 I'm going to hack your Web sites. Both Obama's and McCain's Web sites were taken down.

20:14 It's a good way to get their attention. Then you had multinational network sort of discovery.

20:21 So there's these things called GhostNet out there, which you can research on your own, but 13-plus-hundred systems being compromised...

20:30 ...all interoperating as a network of attacks. What about even more recently, this year?

20:38 Maybe some of you have heard about Google and them being compromised, or admitting to being compromised, at the beginning of this year...

20:46 ...along with about 30+ other large corporations. They were after the company’s source code, which was quite interesting...

20:55 ...because we still don't even know for sure what they were planning to do once they collected that source code.

21:03 So what has this also driven? This has driven active legislation. So our Senate, writing to the president, just on July 1 here...

21:14 ...saying, We have some serious issues with cyber security for our critical infrastructure of the United States.

21:23 So what are some of the issues? So CSI, Computer Security Institute, does a survey every year.

21:30 There are some big jumps right now in password sniffing. Actually, it's easier to sniff than it used to be sometimes, for passwords, and so forth.

21:40 There's nice, little browser plug-ins, be it Fiddler or other ones where you can see all sorts of Web traffic.

21:46 So we've made it user...easier for users to consume that information.

21:51 There's a lot of financial fraud going on, and there's malware infection increasing significantly.

21:58 So what are people doing to try to address these types of issues?

22:03 Well, some of the higher-priority items were log management, so collecting information that's distributed widely over an enterprise...

22:12 ...and then being able to report that in [an] effective dashboard to executive and also management because...

22:20 ...what's happened is that systems have become so complex...

22:22 ...and so many diversified systems trying to keep track of each system individually...

22:29 ...is not a manageable solution.

22:33 So now I'll jump into some security mechanisms that can be deployed across the enterprise with our products.

22:40 So you have authentication, so identifying, hey, is this Bob or Sally that's going to have access to the system?

22:49 Is this Bob or Sally? is really the question. Then for who has access...

22:55 ...Can Bob access this map here but not the other map over there?

22:59 That's called authorization. Then we have a variety of filtering mechanisms.

23:05 So let's say Bob gets into your system...

23:07 ...but now he makes a malicious attack across your wire towards your, let's say, ArcGIS Server.

23:14 What's going to block that? So ideally, having some filtering mechanisms for that.

23:19 Then you have encryption mechanisms to protect that information going across a line or at rest on a hard drive.

23:27 And then you have logging and auditing for what's called nonrepudiation.

23:34 For authentication...So ArcGIS Server has three basic schemes.

23:39 For Web traffic, it has two items; you have Web services and Web applications; those are both circled at the top.

23:47 Then you have this internal communication that's based over DCOM.

23:51 So each of these have different mechanisms to approach. I don't expect you to read this whole chart here in detail right now.

24:00 The key thing is...is that you have different options for authentication, a ton.

24:07 So, if somebody just calls me up and says, "Hey, Mike, can you just quickly tell me...

24:11 ...the authentication option I should be using for my deployment?"

24:15 Well, there's quite a few, so by default, for Web services and applications, no security is used with ArcGIS Server.

24:22 Now you could, let's take IIS, turn on either Basic, Digest, or Windows Integrated the...authentication...

24:29 ...and that results in a little browser pop-up dialog for end users.

24:34 Or on the JavaWorld, you could use containers, then if you have more advanced security con...

24:39 ...needs, you could implement a public key infrastructure...

24:42 ...with client-side certificates and even smart cards.

24:48 Now, the red part here is for specifically only Web applications, so you have .NET form based and Java - - ArcGIS managed.

24:56 Then you have a Web-service-only interface, so it's the ArcGIS token method.

25:02 So why do we have that? It's something to protect across platforms, be it .NET or Java...

25:08 ...be it the SOAP APIs or REST APIs, for providing a common mechanism.

25:15 There's not really a standard that goes across those by default in the IT world at this time.

25:21 And last but not least is that local authentication I mentioned...

25:24 ...with DCOM, which ties in with the Windows Integrated authentication many times...

25:29 ...where you have two groups in the operating system...agsusers, agsadmin...and you really have three levels of access...

25:37 ...none, you're a user, or you're an administrator for those local connections.

25:42 So it's that Web security that gives you that more fine control of role-based access control.

25:51 So where do you store these various users and roles, also called a principal store?

25:56 Well Java has a set of options; .NET has a set of options.

26:00 On the Java side, we start off by de...you def...with...by default with an Apache Derby database.

26:06 You can point it to an Oracle database or SQL, other database vendors; it's up to you.

26:11 There's LDAP infrastructure if you want to utilize that, or even Microsoft Active Directory.

26:17 For .NET security store, by default you have the Windows users and groups; that one creates a little bit of confusion.

26:24 They're like, okay, so is that Active Directory, or is that...is that just my local machine or something else?

26:31 Windows users and groups is a choice for you to use just the loc...a particular machine's users and groups it's aware of or...

26:40 ...a domain's set of users and groups.

26:45 You can also utilize Microsoft SQL Express or the SQL Enterprise Edition out of the box...

26:52 ...or you can implement a custom provider.

26:54 So I pointed to that help document in the Implementation Gallery or that white paper in the Implementation Gallery.

27:02 That was for stepping you through how to implement a custom provider.

27:09 Authorization. So we provide role-based access control with our COTS product to the service level.

27:15 Some of our users want more fine-grained sec...security control than that.

27:21 So Arc...you use ArcGIS Manager to assign various rights to these groups, what they have access to.

27:27 And the services are grouped in folders that have inheritance with them.

27:32 So you can utilize third-party products to get more granular...

27:37 ...so relational databases you can implement role-level or feature-class-level security.

27:43 However, you need to be aware of, if you're doing multiversioned instances...

27:47 ...it can significantly degrade the performance of your solution.

27:51 You also have the capability of utilizing SDE views instead of that.

27:57 So you can also limit the...what's displayed in the user interface.

28:02 So for rich clients, utilize ArcObjects to do that.

28:05 For your Web applications, I actually pointed at that common security code snippet.

28:11 And there's also a nice little tool out there from Microsoft called AzMan; it's basically a[n] authorization management tool.

28:23 So filtering mechanisms. These are primarily third-party options to utilize with our products.

28:28 Firewalls...protecting ports and protocols...access to those.

28:34 A reverse proxy...common implementation option with our products.

28:38 Microsoft now, with 2008, provides code to be able to implement a reverse proxy with IIS.

28:46 Many times, because customers were trying to avoid the cost and overhead of a[n] ISIS Server...

28:51 ...they would implement an Apache solution, instead, on top of it.

28:55 You don't need to do that now for your IT team.

28:59 Web application firewalls. So ModSecurity can significantly reduce attack surface on top of this reverse proxy.

29:07 So ModSecurity is an open source implementation option of a Web application firewall.

29:13 There's antivirus software that you should incorporate on your system, IDS, IPS intrusion protection solutions.

29:20 And you also have this option of limiting acc...applications' access to the geodatabase.

29:25 So you can say arcmap.exe is the only one, only executable...

29:30 ...that's allowed to actually access my database, so independent of the users.

29:34 It's another type of filtering, and that's done by the database tier itself, be it SQL Server or Oracle.

29:44 So a firewall-friendly scenario of implementing our products.

29:49 So I have a couple acronyms here that are not explained, of course, just to keep you on your toes.

29:54 So, in the quest for obfuscation, right?

29:58 So reverse proxy obfuscates internal systems.

30:01 So obfuscation is an interesting one because a lot of security guys say that's not security.

30:08 So what's the purpose of our proxy here? Reverse proxy.

30:13 Well, it can help security...some; it's just the amount of degree that it can help, depending on your configuration...

30:20 ...and how much you supplement it with something like a Web application firewall function.

30:25 So the communication between the proxy and the server, right here, can be on any port that you choose.

30:33 And then, in this case, we implemented a file geodatabase in the...a DMZ.

30:38 Why did we do this?

30:40 Well so, over here, we have our production internal operations, a relational database that's versioned...let's go back...let's see...

30:49 ...come on, one more, there we go.

30:51 And then we take just the default version, send that over to the file geodatabase replicated over there.

31:00 So what we've done is we've segmented datasets that we have, our data-sensitive ones internally...

31:06 ...our ones we want out to the public dataset...

31:09 ...public users out in that DMZ, hey, if they compromise that whole file geodatabase, take that whole thing, so be it.

31:16 But they haven't gone anywhere near your internal operations.

31:20 This is also good for performance, because you can stack a whole bunch of those file geodatabases on each of your...

31:27 ...each server you have...you can have another file geodatabase.

31:30 So you have the read/write capability of a whole new blade for each one of those instances without incurring any special licensing costs...

31:41 ...for a relational database system.

31:45 So for encryption, a lot of third-party options out there too.

31:49 So for the network, we have a, for VPNs, it's common to use...for external users, it's common to use IPSec.

31:58 Some organizations use IPSec for protecting server-to server configuration...communication.

32:06 And then, there's also file-based encryption...

32:09 ...so you can utilize components like, that's called BitLocker from Microsoft or this EFS, encryption file system.

32:18 There's also the capability to use geospatially enabled PDFs combined with certificates.

32:23 So this is utilizing an interesting concept. So I take ArcGIS Server, create a geospatial PDF.

32:30 I can then take that PDF and sign it to say I only allow particular users to be able to open this document...

32:38 ...and they have to have a certificate...

32:40 ...or smart card with a certificate, to be able to view it or do particular functions with it.

32:46 So, and that relies on a public key infrastructure. But so you basically get a PDF lockup information and then hand it out there.

32:54 There's also hardware-based solutions...

32:56 ...so you can purchase now hard drives that encrypt all information written to them on the fly.

33:05 And last but not least, here is relational database management system encryption, so a transparent data encryption, I've talked a little bit about.

33:12 One solution for those remote field operations...people on the desk...out in...doing operations out...complex field...

33:20 ...operations out in the field that need to be locked down.

33:22 You give them SQL Express, implement transparent data encryption, if their system...

33:28 ...somebody runs away with the whole hard drive and system, it's encrypted.

33:36 Enterprise-wide security mechanisms...continuing to logging and auditing, so for nonrepudiation many times, so...

33:44 ...with our products, we have geodatabase history that can be utilized for tracking changes.

33:49 We have the ArcGIS Workflow Manager, previously called JTX, that track...can track feature-based activities.

33:56 And then in 10, we added some new user...a new user tag to track various user requests on the systems.

34:04 So that tag is automatically turned on as soon as you turn on the ArcGIS Server security model now.

34:11 And then, of course, you have a variety of logs out there for Web servers, relational databases, operating systems, and firewalls.

34:19 Okay. So that's plenty of high-level stuff.

34:23 Let's step a little bit into what options are for particular products and solutions.

34:29 So ArcGIS Server secure m...Server security. So as opposed to going through each individual option of ArcGIS Server security model...

34:38 ...I'm going to ask questions that some of our customers are...seem to be not clear on what's going on...

34:45 ...or what things are configured by default, let's say.

34:49 So who...who here believes communication with ArcGIS Server's Web services are secure by default?

34:59 Oh, good, so we're communicating well. So, no, it's not.

35:03 Communication via ArcGIS Server and all clients are clear text by default.

35:07 Secure Web communication, you can ideally utilize an SSL cert. to secure that.

35:13 For those DCOM local communications, you can use IPSec tunnels between those systems...another interesting one.

35:22 So I have a large Internet provider solution, and I'm exposing Web services out there with

ArcGIS Server.

35:33 Do I need to have a reverse proxy in that implementation?

35:37 Who says...so is a reverse proxy required, yes or no?

35:43 If you believe a reverse proxy is required, please raise your hand.

35:49 Okay, we have a couple people. So the actual answer is no, it's not required, and not even for security.

35:58 So some customers implement a reverse proxy to eliminate DCOM traffic across firewalls within their internal operations.

36:06 So a particular security group might make it a requirement, but it's not a requirement to implement a secure solution.

36:16 So, when used with a Web application firewall, that's when you really start improving the security function of a reverse proxy.

36:27 So is there security hardening guidance from Esri?

36:30 So I need to lock down my operations; how do I do it?

36:33 Or I keep on configuring ArcGIS Server, and my IT group says I have to do these particular things...

36:39 ...I do it, and it falls over. Is there some basic guidance?

36:42 The answer is yes.

36:44 Go ahead and check out the Enterprise Resource Center Implementation Gallery.

36:48 We'll be updating this security guidance before the end of 2010 with the version 10 and Windows 2008.

36:56 Let me know if you have other particular implementations you need guidance on.

37:04 Another interesting one.

37:05 Should I assign the everyone group in...to the root in ArcGIS Manager? What does that mean?

37:12 Okay, well, I set up ArcGIS Server; by default, it doesn't have this security function turned on.

37:19 So I go ahead and turn on this security function, which some of you probably have done, and all of a sudden, nobody can access my system.

37:27 So what does somebody do in response?

37:29 They take the everyone group and put it into the root.

37:32 Now, what have you done?

37:34 You've just all of a sudden converted your system back to everyone has access to your system

again for everything, by...by default.

37:41 Now, some people want that model, because it does make it easier to use.

37:46 So this is...I didn't even have you raise your hand on that one because it really depends on what your needs are, right?

37:53 A lot of our customers have a basic security need; they don't have this medium or high security need.

37:58 So ease of use is extremely important for some of our customers.

38:03 So this basic security model...it's an okay implementation option, but it's not really recommended for standard or advanced.

38:10 The common security practice is deny by default in higher-risk environments.

38:18 So can I provide security more granular than the service level, yes or no?

38:23 If you believe yes, raise your hand.

38:28 Okay, so we've got half the building, and maybe the other half is asleep; I don't know... can't judge that easy enough.

38:35 Yes, you can; right now, you have these SDE views or third-party software relational database components, and so forth, to help supplement that.

38:45 We also have this other future option we're working on, this integrated security model...

38:49 ...being able to pass user context from Web server to application server to database server tiers.

38:56 So briefly, what is this new integrated security model?

39:00 As I mentioned, the user context passes through; what's the big deal?

39:05 So it allows you this more fine-grained access control, role-level security; it also can provide you a single interface for HTTP and DCOM connections.

39:15 It also can improve your capabilities for nonrepudiation throughout your environment.

39:21 Current release status of this is we're collecting more customer use case information.

39:26 Validation of this will potentially lead to production support...

39:30 ...but we have some outstanding concerns of the performance, security, and usefulness of this solution.

39:36 That's why we're still in this mode of working with the customers to refine this.

39:41 What are some of the main scenarios it addresses?

39:44 As I mentioned, centralized security management...

39:47 ...so both local DCOM and Internet connections managed from the ArcGIS Server management interface...

39:53 ...utilizing Windows integrated security.

39:58 So right now, you manage those two levels of security, your local connections and your HTTP connections...

40:05 ...completely independently from each other.

40:08 But this model could change it.

40:11 So you also flow the Web user identity to your database via what's called a proxy user.

40:16 So this is a relatively newer technology in database systems...

40:20 ...that you don't establish a separate session to the database for every user accessing the system.

40:27 So you sort of can lump user accounts through, but you add a sort of a...like a WHERE clause onto it saying...

40:33 ..."where the user is John,"...

40:34 ...or "where the user is Bob," using that same connection.

40:38 So it allows you the capability to make a lot more scalable type of solution.

40:43 So this will allow for logging functions...

40:46 ...nonrepudiation across all the architectural tiers in high-security types of environments, those advanced security needs.

40:53 It also provides that role-level security function we talked about.

40:57 You also might want to implement a custom server object extension...so...to make use of, hey, it...

41:03 ...now that I know a particular user is using this particular function with ArcGIS Server...

41:09 ...I could potentially implement feature-level security doing that.

41:16 So what does integrated security look like, providing role-level...and role-level security?

41:22 So in this case, the user is logged in as administrator; I see both red and green lines.

41:28 When I log in as just plain old Mr. other user, just Joe user, I...those red lines magically disappear.

41:37 So it's a single Web service that the database has now...because it knows of particular users...

41:44 ...it knows to not be able to provide particular information back to the end user.

41:49 One of the issues here, of course, is that, in this case, for a roads network, lack of information

implies...

41:55 ...you know, the mind can sort of fill in the gaps in some of these road networks...

41:59 ...that something interesting is occurring along those road networks that I'm not allowed to see.

42:05 So desktop security. This client typically has the most access to sensitive datasets out there.

42:14 Now, the reason that's historically not been too much of an issue is it's in a more secure environment.

42:20 It's not exposed out there on the Internet for everyone to access anything.

42:26 So you have a variety of system connections.

42:28 You have direct connect to the relational database management system via standard SQL calls...

42:34 ...you have application connect to SDE, and you have HTTP service request, geodata service, and so forth.

42:40 You also have integration with the token service and Windows native authentication.

42:46 You also have ArcObjects development options [available] to you...

42:49 ...and you can record user-initiated transactions, fine-grained access control...

42:54 ...such as edit, copy, cut, paste, and so forth.

42:59 So the one that's sort of interesting here is geospatial cloud computing, or hopefully the other ones were interesting too...

43:05 ...depends on your mind-set.

43:07 So, question for to...today, a real nice, easy one...so who here thinks cloud computing is safe?

43:16 Raise the hands...so I got...I got two hands...one and a half hands.

43:23 Nobody else thinks cloud computing's safe?

43:26 It really might not be that bad. So, the answer...it depends.

43:32 You like that? And we'll just leave it at that?

43:36 What does it depend on? So cloud computing actually has some interesting security benefits...

43:42 ...and I got some of my information also from some research that...that the government's been working on too.

43:50 So virtualization and automation...automation of systems... What does that result in?

43:56 Well, I'm able to take standard images and stamp those out on a whole bunch of systems...

44:00 ...I don't have to rebuild each system from scratch.

44:04 So for security, I can make a whole bunch of systems identical quickly, easily.

44:11 You also have broad network access.

44:13 This was an interesting one that came up that said, hey, now that I can access my same information here as I can in my office...

44:22 ...I don't necessarily need to carry around a USB key to transfer datasets...

44:26 ...those nasty USB keys, carrying viruses and everything.

44:31 So there's also this idea of segmenting datasets...using the public cloud to your advantage.

44:37 But you say, Well, public cloud, what should I keep out there?

44:40 Well, how about public datasets?

44:42 Keep those in the cloud, and then your internal operations, you keep your sensitive datasets.

44:48 So it's not like an all-or-none type of thing. Talk more about that _____ soon.

44:53 So there's also potential economies of scale.

44:56 So you have lower-cost backups...it's lower cost to back up your datasets out there because of their infrastructure.

45:02 And then you have various self-service technologies available to apply security controls on demand...

45:07 ...be it a...a...their simple firewall control changes, or so forth.

45:13 So what are some of the risks of implementing into a cloud?

45:18 So first is vendor-practice dependence. It's now dependent on what the vendor, the cloud vendor, is doing.

45:26 So there's potential substandard security controls out there resulting in vulnerabilities.

45:32 There's also a little bit of the loss of governance and control.

45:36 Sometimes, why, I don't know where my dataset's going to be.

45:39 I specifically don't know what machine it's going to be on; sometimes I might not even know what country it's going to be in.

45:47 Vendor lock-in...so this is an interesting one too...so we have...

45:51 What happens with your datasets once your services are terminated?

45:54 Some cloud providers write up their requirements pretty clear; other ones, it's a little bit more agile, we'll call it.

46:03 So be aware.

46:07 There's a lack of tools, procedures, and standards to ensure portability...

46:10 ...so I cannot easily take my image that I make for one cloud provider...

46:16 ...and roll it out into another one.

46:19 So if I create an AMI with Amazon, I can't roll that out into any other cloud provider other than Amazon.

46:27 Now there's advantages for Amazon too; I'm not bashing them, but just an example.

46:32 And you can also be hostage to the vendor cost increases.

46:35 This is a concern of the governments, too, saying, well, okay, so now...

46:39 ...you're saying you're a vendor; we don't have to hire as many IT guys...

46:43 ...you're going to do a lot of those functions for us...we get rid of these IT guys.

46:47 Now you decide to dramatically raise your rates. I can't pull that back away to my IT group because they're nonexistent.

46:55 They don't know how to do this stuff anymore.

46:58 So anyways, it's an interesting phenomenon, and it's just that loss-of-control concern.

47:04 There's also the sharing of computing resources, also called multitenancy.

47:09 This is where you can have intentional, or unintentional, gaining access to other users' data out there.

47:16 There's also unclear responsibilities during security incidences right now.

47:21 So who's in charge of the forensics process?

47:24 Are you, as a customer of a cloud solution, allowed to follow that forensics process or help facilitate that?

47:29 Will you have access to anything to help facilitate that?

47:34 There's also increased data being transmitted across a wire.

47:38 That same thing I said that was an asset for that USB scenario is also potentially a risk.

47:44 Because now you're sending more data, you've now increased your disclosure risk.

47:51 And of course, there's the...the threat exposure varies upon what's called a deployment model; I'll talk about those briefly.

47:59 But you have a private cloud, which has relatively lower risk of...of threat exposure.

48:05 You have community, and then the highest threat exposure is in the public cloud.

48:09 Those are all relative.

48:13 So these...what about the service models, and how do they affect an organization?

48:19 So I have Infrastructure as a Service; I didn't put the expand out, these acronyms to the right because...

48:29 ...I really translated it to what it means to a security guy, or a person trying to implement a solution.

48:36 Infrastructure as a Service...what does it mean?

48:39 I get administrative access of [to] the operating system and all the software that's deployed on that VM.

48:44 So now I'm managing that; I'm responsible for the security of that operating system...

48:49 ...and the configuration of it, and every single software component on it.

48:53 So ArcGIS Server for [on] Amazon EC2 provides you an Am...

48:58 ...AMI, it provides you the operating system, the software, ready to roll...

49:04 ...but who's responsible now, as soon as you get that up and running...

49:07 ...for managing the security of it, locking it down, and so forth?

49:10 It's the customer.

49:12 So we also have customers implementing...

49:15 ...be it with Terremark, and we also have various private cloud implementation going...options...

49:19 ...on...customers implementing private clouds right now.

49:24 For developers, they have this thing called Platform as a Service.

49:28 So Esri, we provide up...these various Web mapping APIs out there...JavaScript, Flex, so forth.

49:34 Microsoft has their Azure environment.

49:37 Some of our customers have implemented ArcGIS [API for Microsoft] Silverlight applications in the Azure environment.

49:46 And then, there's the end users...Software as a Service (SaaS).

49:50 So this is where, basically, I don't want to administrate, I don't want to develop, I just want to use the software.

49:57 ArcGIS.com is an example, the sharing environment, Business Analyst Online, and ArcGIS Explorer.

50:06 So the cloud deployment options...talked a little bit about those a bit...little bit ago.

50:11 So it's about location.

50:15 So a public cloud implementation...Amazon hosts it; they're doing everything for you with the

systems out there.

50:21 Private cloud, you're going to do that in your internal corporate infrastructure.

50:26 There's also hybrid and community, and all those, there's mishmash, but those are the two extreme.

50:31 Somebody else completely does it, and the house and all the infrastructure are really, you are doing it...

50:36 ...yourself, and your internal operations.

50:39 What is the primary driver between this public and private deployment? Security.

50:45 So back in the...just well, last month, IDC did a survey of IT executives saying...

50:52 ...Okay, so is there a preference for using a private cloud versus a public cloud?

50:57 So 55 percent said, Hey, a private cloud was more appealing than a public cloud.

51:03 And 22 percent said, you know, Roughly a wash.

51:06 So one interesting thing I got out of this is that it's not like a cloud implement...

51:12 ...a cloud implementations are going to be one particular path or direction for public or private.

51:17 You're going to see a mix from within organizations.

51:23 So one of the things I talked about earlier was assessing your particular security needs.

51:28 Same thing needs to be done for cloud computing.

51:31 For your data sensitivity, understanding, Is it pum...public domain information?

51:35 Is it sensitive that I need to keep track of closely?

51:38 Or is it classified?

51:40 Identify my user types, be it public or internal users. And then categorize your solution accordingly.

51:46 Same type of security pattern of basic, standard, advanced.

51:50 Now most public cloud implementations are basic at this time.

51:54 Think of the security model similar to social networking sites such as Facebook...

51:59 ...which hopefully you're aware of periodically gets hacked.

52:03 Most...some people...well, so that's a funny one, right?

52:06 So I gave an analogy of, you know, cloud computing...

52:11 ...public clouds being analogous to a social networking site like Facebook, and they said...

52:16 ...Wow, that's the best thing ever; I've never seen that or heard of any issues, and I'm like, okay, you know, just be aware.

52:24 Most GIS users will have only basic security needs though. So, I mean, it's...

52:30 ...you can worry a lot about risk and, you know, solutions, but...

52:35 ...how...how much is it relative...how much are you concerned, with your organization, about those risks?

52:41 So some interesting topics out there...I talked about data location.

52:45 An interesting one that comes up for international organizations is the Patriot Act.

52:50 They say, okay, so you're saying, hey, if I give my data into the Google's cloud...

52:55 ...Google can't promise me where that data live[s] or resides.

52:58 If it happens to end up in a server in Kentucky that the government could technically, at any point in time...

53:07 ...say it's their data to read, the United States government.

53:10 Gets the inte...international customers little bit concerned.

53:14 Some cloud providers don't assure location.

53:17 So Amazon currently provides a mechanism to say, yes, we'll keep your data at this particular location or a country.

53:26 Google currently, from my latest understanding, does not do this, at least yet.

53:32 Identity management is another tough area in cloud computing that's to be addressed.

53:39 So there's a long-term vision formulating a national security strategy for trusted identities...

53:44 ...was just released at the end of last month, but this has got a long ways to go.

53:51 And why is identity important?

53:53 Well, if we look at the compromises of Google and other environments just in the last year...

54:00 ...we weren't able to identify who those people were that did the compromise to our solution...

54:06 ...due to a lack of identity management.

54:10 So a shared responsibility model...this is something that's core to cloud computing.

54:15 The cloud provider is not taking full responsibility for the solution gets...[getting] implemented.

54:20 It's shared. The customer takes some; cloud provider takes another part.

54:25 However, the details of who has responsibility for what is not very clear many times.

54:32 So this makes it also very difficult for aligning with the regulatory compliance...quite questionable.

54:42 So what's some best practice guidelines for implementing solutions in the cloud?

54:47 Well, if your security model is beyond basic, then you need to start thinking about the same ideas of breaking up tiers...

54:54 ...such as shown in this diagram...Web app, database.

54:58 You want to protect your da...information in transit across that wire, and you also want to protect information at rest.

55:05 That's a key one for cloud computing and customers more concerned about how to do security, you know...

55:12 ...in decent format in cloud computing.

55:16 So what you could do is encrypt your information at your site in your organization before sending it into the cloud.

55:24 It remains encrypted out in the cloud until it's actually served out to the end user.

55:29 So the cloud pro...provider doesn't have readily available access directly ever to that dataset.

55:36 Credential management...I talked about the importance of that. You also might want to implement the built-in firewall...

55:43 ...operating system firewall capabilities.

55:45 And there's also the ArcGIS Server application security model; it can layer on top of that.

55:51 So ArcGIS Server on Amazon EC2. So the default deployment, what is it, out of the box?

55:58 You get this AMI, which is a confi...configuration of ArcGIS Server, Windows 2008, and has a file geodatabase...

56:08 ...so all your tiers are really combined.

56:11 Now we provide some scale out guidance in the help along with that, and you can look that up on the Web.

56:18 But what about the supporting infrastructure behind this? How does... When I have that number of VMs starting to spin up...

56:24 ...so four, five, six VMs starting to spin up in that environment...

56:29 ...how do I ensure that those are all secured in a relatively effective fashion?

56:35 Many people are setting up this RDP thing, remote...

56:37 Okay. So you want to minimize your administrative attack surface across these virtual machines.

56:43 So if you have a Windows box, users commonly ought... log in via what's called RDP, Remote Desktop Protocol.

56:51 But you don't want to necessarily expose this on all your servers, because it's sort of, you know, the keys to the kingdom.

56:59 So what you can do instead is set up a management instance in front of all your servers...

57:04 ...and then your back-end servers can talk amongst themselves...

57:06 ...and you talk to the other servers through that single management instance.

57:12 So what if you wanted to get into more advanced single sign-on integration in cloud computing with your operations right now.

57:19 So Amazon has this virtual private cloud implementation of VPC where you create an IPSec tunnel between your internal app or...

57:28 ...enterprise and the cloud implementation.

57:31 You really don't have to do much special to accomplish this...

57:35 ...because it just ties in with Windows integrated authentication across that tunnel.

57:41 Now what if you don't want to have that VPN tunnel in place...I want to have more of a federated solution?

57:49 So this is where...use a[n] Active Directory Federated Services.

57:55 So in this case, you have a browser making a request against Windows Identity

58:02 Identity Foundation says, hey, you don't have the token that I need to get access.

58:06 Browsers bounce back to his system, goes against the ADFS server, Active Directory Federated Services.

58:13 It's the domain controller, has now a token to pass on to the browser; browser then passes it on to this little agent in front of the product...

58:23 ...and then you have some security in front of it.

58:26 So this actual scenario we're working on validating.

58:32 Amazon actually has worked with Microsoft to do a pretty good write-up of four or five different scenarios over the last couple months.

58:40 So there's some links to those guides later on in this presentation.

58:45 So some product-specific guidance...ArcGIS Server for...on Amazon EC2.

58:49 You get an AMI that's not hardened beyond the Windows 2008 server defaults.

58:55 We're looking into potentially providing a security-hardened AMI.

59:00 You need to tell me your benchmark requirements for that, so if you have a strong need for that, let me know.

59:07 There's also basic Esri online help guidance...

59:11 ...and Amazon has that security best practices guide that they released at the beginning of this year.

59:18 For the ArcGIS.com sharing environment, Arc...

59:21 ...there's online help for sharing in content, parti...participating in groups, similar type of security model as Facebook.

59:29 We recently went through a SAS 70 review of Esri's hosting services...

59:37 ...to help ensure we're providing the right type of robust security environment for your needs.

59:43 And we have an upcoming Esri geospatial cloud security...cloud computing security white paper coming out.

59:50 Hoping to get that out before the end of 2010.

59:55 So with that, enough of cloud computing.

59:58 So a little bit about mobile phone security.

1:00:01 So with more platforms, be it ArcPad, Mobile, iPhone, Android...more functionality, larger user base...

1:00:08 ...this leads to increased hacker attention, so this is an interesting spatial analysis of hacking attempts.

1:00:14 Via one, on the left, is via Bluetooth, so what you'll see is that...

1:00:20 ...in Bluetooth, it exponentially grows once it hits a densely populated area...

1:00:25 ...it's proximity-based attacks. Bluetooth, you need to be within...I don't know...is it 20...20 yards of another phone for it to attack...

1:00:36 ...versus a message which you could send out to a whole bunch of systems...

1:00:39 ...which would be more distributed widel...in a wider scenario.

1:00:43 It's not dependent on a population density.

1:00:48 Mobile phone security, so for ArcPad. You have this AXF data file for password protecting, encrypting it.

1:00:55 You have the individual memory cards, SD memory cards; you want to encrypt those.

1:01:00 ArcGIS Server has user[s] and groups; you want to limit the publishers of that.

1:01:03 You have various interconnects...

1:01:05 ...Internet connections out there; you want to secure the ArcPad synchronization traffic occurring.

1:01:12 For Mobile, you have that geodata service, you can utilize SSL; VPN tunnel's another option.

1:01:18 About 10 to 20 percent of our customers use VPN tunnels.

1:01:22 Utilization of the token service can be incorporated, also for Web services you can prodect...protect via credentials...

1:01:31 ...or filter by the operating system, the IP of the device.

1:01:34 There's also a unique identifier on each one of these mobile devices.

1:01:39 And if you know much about security, you would know also like...

1:01:43 ...all the iPhones' compromise was along that same unique identifier...

1:01:48 ...not iPhones. That was the iPad, wasn't it?

1:01:51 The iPad attack was all based on the unique identifier...getting everybody's e-mail addresses of whoever had an iPad and that.

1:02:00 So encrypting data at rest...you can also do that via the Windows Mobile Crypto API.

1:02:06 And there's a variety of third-party tools for encrypting the entire storage system.

1:02:12 So hopefully, I didn't rush you too much, but...

1:02:17 So in designing an enterprise GIS security strategy, you first need to start out by identifying your security needs.

1:02:24 Assessing your environment and starting to map out how you fit relative to...to these patterns that I've talked about today.

1:02:31 You need to understand your current security trends, what's going on on there, what might be affecting you over the next year...

1:02:37 ...or two or three...understanding your various security options.

1:02:40 Go ahead and check out the Enterprise GIS Resource Center...

1:02:43 ...for enterprise-wide deployment mechanisms and application-specific options...

1:02:49 ...and then implement security as a business enabler. Improve...you want to improve appropriate availability of information.

1:02:56 Your goal is not to be the wet blanket in the organization, locking everybody down.

1:03:04 So if you need more information on the technical specifics of how to implement ArcGIS Server's security function...

1:03:12 ...there's a Microsoft .NET Framework session on Wednesday and Thursday.

1:03:17 Java session was canceled but we'll be posting the...into the Enterprise Resource Center a link for the DevSummit presentation for Java.

1:03:26 And we also have a Professional Services offering for a[n] enterprise GIS security review.

1:03:33 A variety of resources that I won't have you go through right now because that would be quite intense.

1:03:40 But I would like to leave it open for making sure I get from you as much as possible where you need to hear more security guidance out of Esri.

1:03:51 And that is it for today, thank you.

© Esri 2013 http://www.esri.com