# Remote Access and VPNs Part 2 of 2

## Table of Contents

- Remote Access ................................................................................................................................ 2
- Identification and Authentication Methods ................................................................................... 3
- Remote Access Example -1 ............................................................................................................. 6
- Remote Access Example -2 ............................................................................................................. 7
- Access Control Servers .................................................................................................................... 8
- Virtual Private Networks (VPNs) ..................................................................................................... 9
- Remote Access Example -2 ........................................................................................................... 10
- Virtual Private Networks (VPNs) ................................................................................................... 11
- Remote Access Example -2 ........................................................................................................... 12
- Virtual Private Networks (VPNs) ................................................................................................... 13
- Remote Access Protocols .............................................................................................................. 15
- PAP – Password Authentication Protocol ..................................................................................... 16
- CHAP – Challenge Handshake Authentication Protocol ............................................................... 17
- EAP – Extensible Authentication Protocol .................................................................................... 18
- Network Information Services (NIS / NIS+) .................................................................................. 20
- Notices .......................................................................................................................................... 22
Remote Access

Remote Access

Allows users access to a network from outside the traditional boundary of the network

Identification and authentication are critical

- Identification – establish the identity of a remote access user
- Authentication – verify the identity of a node or end-user

Node authentication

- Verify the source host (device) attempting remote access
- IP address, hostname, may even include key files

End-user authentication

- Verify the identity of a user
- Multi-factor authentication may include passwords, PINs, key files, or biometrics

**180 Okay, switching gears to remote access, we allow the users access to the network from outside the traditional boundaries of the network. We’re talking about what we would normally call an extranet at this point. But that’s not what it is. It’s end users anywhere on the planet deciding that they want to dial in and get a hold of resources that are our enterprise.

And so, what we need is we need good identification of those people and good authentication. Remember, identification asserts that they are who they say they are and authentication is the proof of that
assertion. That’s verification of both the computer and the user in a lot of cases.

We could do node authentication, which is the individual computer. But I’d also like to do end user authentication because that end user could be using a machine that is compromised. And it may be that our security policy says that they have to be on a company asset using a company computer and being themselves. They can’t impersonate at that point.

**Identification and Authentication Methods**

**Identification and Authentication Methods**

**RADIUS / TACACS+**
- Centralized authentication and user management
- Servers verify user and approve remote access

**Thin Clients**
- System architecture where user’s computer has limited capability
- All processing occurs on centralized remote access servers

**Remote Access Servers**
- Provides desktop environment to thin clients
- Examples: Microsoft Terminal Server, Citrix Server

**181 So, what could we use for**
identification and authentication methods? What systems could we put in place? Well, the two majors here are RADIUS and TACACS. I think that those are the most reasonable. And we’ve talked about them at length before. One of the other things that we could use is some sort of thin client, some system architecture out there that limits the capability. In other words, making sure that when they’re doing this that they authenticate with us. But they are also limited to a subset of commands.

So, I like the thin client idea. These are usually called terminal emulation. There are a whole host of providers that do this out there today. You can pick your provider out there. But I really think that Novell used to be really great at this. Their ability to actually get connectivity for those clients to use a centralized server for any of those activities was awesome.

And the proof that I offer was Novell compared to everybody else when it came to printing. If you actually tried to do printing on a thin client from Novell, you could actually print here to this printer here. But if you did it on anybody else’s client, if you wanted to print here, you had to send all of your printer information up the channel and then back down the channel. Or worse, and this happened a lot of times, was when you went to print you printed on a server at the headquarters. And so, I don’t think that’s a good way to go. But Novell had figured that out. They
could actually redirect that traffic and make it work here. They had a really amazing print profile set up for that particular purpose. So, I like their thin client.

I'm sure that there are other better thin clients today. But I think we're moving more toward a cloud computing environment. So, I think a lot of this is washing away.

And we could do remote access servers themselves. Remember, where are your authentication credentials being sent? And who's doing the authentication on them? The Citrix server and the Microsoft Terminal servers will also-- would do this for you. I think Microsoft has a really robust implementation of RADIUS that I like for the choices that we're doing here.
**182 Okay. So, let's talk about a couple of remote access examples here. So, we start off with the remote user doing some sort of authentication. Whatever that authentication is we're sending it over the Internet. Of the three protocols that we have here, probably CHAP and PAP-- well, I think that they're unencrypted, so don't think that we should be sending them. But this is what happened in the past.

Okay. We'll probably use EAP today. Then we bounce to the remote access server. And then the remote access server actually does the
authentication for us. The username and password is passed across here. So, we need protection here. We need encryption and communication there. So, we're going to look at each one of those.

Remote Access Example -2

Remote access security issues

- Replay attacks – attacker captures credentials from a previous session and attempts to use them again
  - Timestamps in credentials
  - Nonce (random number used once) in credentials
- Password guessing
  - Multi-factor authentication

**183 So, the security issues that we run into here are where are the credentials being passed? Are they being passed in the clear? Can they be replayed at a later point in time? Can there be multifactor authentication put in place to stop the password guessing? I think tokens, multifactor authentication, is your best friend.
Access Control Servers

Access Control Servers

RADIUS
- UDP based solution, sometimes built into routers
- Passwords kept in plain text on the server, but encrypted on the wire

TACACS+
- TCP based, Cisco proprietary solution
- Password always stored / transmitted in encrypted form

Diameter
- Extension of Radius
- Clients request authentication, servers process them, agents forward or proxy requests to a server

**184 Access control servers, we’ve talked about RADIUS and TACACS. Remember RADIUS uses UDP, TACACS uses TCP. You go, “Okay well what’s this DIAMETER thing?”**

Well, the name of DIAMETER is actually a joke because what they said was DIAMETER is twice the

Now, here's the thing. I think DIAMETER is a better protocol because not only does it do UDP, but it also does TCP. And everything that’s implemented in DIAMETER is borrowed from RADIUS if you will.

I think it’s kind of like IPsec. Why don’t people use IPsec? Well,
because it’s got so many configurations on it it’s confusing to those people. So, I think DIAMETER is a good protocol. I don’t think that it’s used that much today.

**Virtual Private Networks (VPNs)**

**Virtual Private Networks (VPNs)**

VPNs secure data sent across un-trusted networks.

- Allows secure communication without dedicated lines
- Can use existing Internet connection; replaces dial-up modems
- Open Wireless networks
- Security depends on the VPN implementation
  - Strike a balance between speed and strength of encryption

**VPN concentrators**

- A dedicated device that processes VPN connections
- Examples: Cisco, Juniper

The end-user host is an attack vector - the VPN does not protect the end-user host – only the data it sends over the wire.

**185 Okay. Virtual private networks, again, secure data is sent across an untrusted network. So, therefore what we need to do is encrypt those communications. It could be being sent over and open wireless network, so therefore we need virtual private networking as we saw on the diagram.

Let’s go back to the diagram.
Remote access security issues

- Replay attacks – attacker captures credentials from a previous session and attempts to use them again
  - Timestamps in credentials
  - Nonce (random number used once) in credentials
- Password guessing
  - Multi-factor authentication

**183 As we saw here, we might need virtual private networking right there so that nobody can see what’s going on.**
Virtual Private Networks (VPNs)

VPNs secure data sent across untrusted networks.

- Allows secure communication without dedicated lines
- Can use existing Internet connection; replaces dial-up modems
- Open Wireless networks
- Security depends on the VPN implementation
  - Strike a balance between speed and strength of encryption

VPN concentrators

- A dedicated device that processes VPN connections
- Examples: Cisco, Juniper

The end-user host is an attack vector - the VPN does not protect the end-user host – only the data it sends over the wire.

**185 When we secure that data across the untrusted network, then that means that we've got to do all the setup. And that could cost from a security and administration standpoint.

Next is what we call VPN concentrator. A VPN concentrator is nothing more than--
Remote access security issues

- **Replay attacks** – attacker captures credentials from a previous session and attempts to use them again
  - Timestamps in credentials
  - Nonce (random number used once) in credentials
- **Password guessing**
  - Multi-factor authentication

---

**183 This end point here for all the different remote access clients that are out there to dial into. It is an aggregation of all of those end point tunnels that are out there.**

---

---

---
Virtual Private Networks (VPNs)

VPNs secure data sent across un-trusted networks.

- Allows secure communication without dedicated lines
- Can use existing Internet connection; replaces dial-up modems
- Open Wireless networks
- Security depends on the VPN implementation
  - Strike a balance between speed and strength of encryption

VPN concentrators

- A dedicated device that processes VPN connections
- Examples: Cisco, Juniper

The end-user host is an attack vector - the VPN does not protect the end-user host – only the data it sends over the wire.

**185 I like a lot of VPN concentrators that are happening today because of our mobile workforce. I really like one from a company that-- well it's Cisco. And they use something called Get VPN. The reason why I like it is because the concept of the protocol, or the concept of their implementation of VPN, is that they can pop up these clients. Those clients can all get keys and create a quick network that they're using for their communication. And then when they dissipate, and they go their way, and the go on to another team, they can all pop up again and create another set of keys that is used for that
particular session or for that particular project. And it's very easy on the client.

Not only is it easy on the client, what I find truly amazing is that it works across almost all hosts that are out there that are-- all tablets and all operating systems that are out there. I think it works on the Apple and the Android all the way up to like one version ago, which I find really amazing. So, I really like that as a tool because the big tough problem with VPN concentrators and VPNs in general for clients is actually getting these things set up. And they've made that ease of implementation with the robustness of security still in it.

Remember the end user, they're an attack vector. It could be that you could actually compromise their physical machine and then lie resonant as an attacker on that machine, and wait for them to connect up over the VPN connection, and then steal all that information and toss it back out the door. And this is why I say maybe you ought to think about multifactor authentication.
Remote Access Protocols

Password Authentication Protocol (PAP)
Challenge Handshake Authentication Protocol (CHAP)
Extensible Authentication Protocol (EAP)
Network Information Services (NIS / NIS+)

**186 Some password protocols, remote access protocols, that we need to pay attention to, PAP, cleartext, challenge handshake authentication protocol, extensible. And then we'll talk about NIS and NIS+.**
PAP – Password Authentication Protocol

Sends username and password in the clear
Passwords encrypted on the server
Standards-based protocol supported by many vendors
No replay attack protection
Authentication ONLY at initial connection

**187 So, PAP is clear text. Clear text is probably bad. Now, we used PAP in situations where we controlled the wire between us and both end points. PAP was used in the days when point to point protocol, where you actually dialed up to your ISP and said I’d like to authenticate. We don’t do a lot of that these days.**
CHAP – Challenge Handshake Authentication Protocol

Authentication at initial connection and anytime after that

Passwords unencrypted on the server

- Microsoft’s implementation, MSCHAP, encrypted passwords on server

Replay attack protection through use of nonces

**188 CHAP, challenge handshake authentication protocol, does not send the protocol across the wire. What it does is it takes the password that’s supposed to be sent, and it hashes that information. It does a challenge nonce from the server. So, the network server receives the challenge-- I mean sends the challenge. And the remote user takes that nonce and that password, combines them together, and passes back a hash that is valid for this particular session. I think that that is an amazing way to do it.**
EAP – Extensible Authentication Protocol

General purpose authentication protocol

Similar to CHAP, but supports many authentication methods
  • Includes multi-factor authentication

Can be extended as new authentication methods are created

Used widely in wireless (802.11) to authenticate users

**189 Enter what we want today.
The word extensible is really the key here. That means that today we use it this way and tomorrow we can extend it to something else. We can pull out this thing that doesn’t work and put in a new thing that does work. In extensible authentication protocol what we say is this is how we’re going to communicate back and forth between each other in a wired or wireless world. Each way works. And what we’re going to do is once we set up this general session between us, whatever the authentication mechanism that we’re using today, if it works, and it’s secure, we’ll keep on using it. But if
tomorrow we're susceptible to--and I'm making something up here. Tomorrow our extensible authentication protocol that we were using is susceptible to some variant of Heartbleed. And I'm just making that up because it's something new and people understand it. If it's some variant of-- if it's not good anymore, then what we can do is then say we're going to pull that piece out. And we're going to put in a new authentication protocol that's going to work.

Extensible authentication protocol is a carrier for authentication that makes it so that the communication from remote user to network access server is-- well, it's clean and neat and also means that our adversary can't break in to it. And if they break into it, we can change it. This means that once we put this infrastructure in place, once we have EAP running in place, we can change out different pieces of it.
Network Information Services (NIS / NIS+)

Shared database authenticates to services and systems

Supported by all major *nix systems

Passwords encrypted on the server

NIS+ adds

• MD5 hashed passwords, access restrictions, and uses Secure RPC for communication

Authentication process

• User sends username and password to NIS client.
• NIS client requests username and password from NIS server.
• NIS client compares what the user provided to response from NIS server.

**190 Switching gears here, and remember, we're talking about remote access to stuff, to business stuff. What is that stuff? Well, it could be file servers. With NIS and NIS+, what we find out is that this is a wonderful tool for getting access to another server on the other side. In NIS+, what we did was we said well, with NIS it's clear text passwords. We could do impersonation here. So, we probably don't want to do that. So, what they did was in NIS+, they added more to it.

What did they add? Well, they added MD5 hash on passwords.
They added
access restrictions. And in the implementations, they used secure RPC if you actually needed it, depending on the implementation.

In the authentication process, the user sends the username and password to the NIS client. Bad. NIS client requests username and password from the NIS server. Bad, because it's clear text. NIS client compares what the user provided to the response from the NIS server. Okay, that's potentially all clear text.

Now, the bad thing about NIS, I believe I talked about this before, is that it's backward compatible so that we go from secure NIS+. And the client says, "Well, I'm stupid and old and I want to give you a clear text password." It says, "Okay, I'll take it," because I want to satisfy their requirement. So, NIS-- NIS+ is backward compatible and therefore will dumb down to the lower level and is susceptible at that point.
Notices

Carnegie Mellon University

Copyright 2018 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution. This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study. Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu. Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

DM16-0056