Chapter 52
Routing

- Packets on the Large.

DeepSec Vienna 2007
7 Layers of Insecurity

Copyright Information

DeepSec Vienna 2007
7 Layers of Insecurity

Chapter 51
Routing

- Agenda
  - Attacks on Routing Protocols
  - Attacks on forwarding

DeepSec Vienna 2007
7 Layers of Insecurity

Attacks on Routing Protocols

- Routing is no Heaven

Spoofed Routing Updates

- Modifying routing tables
  - Simple on RIP/EIGRP
  - More Complex on OSPF
  - Unlikely on BGP
- Redirect user traffic to attacker
  - MitM
  - Stealing data

DeepSec Vienna 2007
7 Layers of Insecurity

Attacks on forwarding

- Is the way to Amarillo?

Source Routing

- The Path is in the Packet
  - Not disabled in most networks
  - Spoofed two way communication
  - Bypassing established Paths
- Risk high, Impact high

Chapter 51
TCP/IP

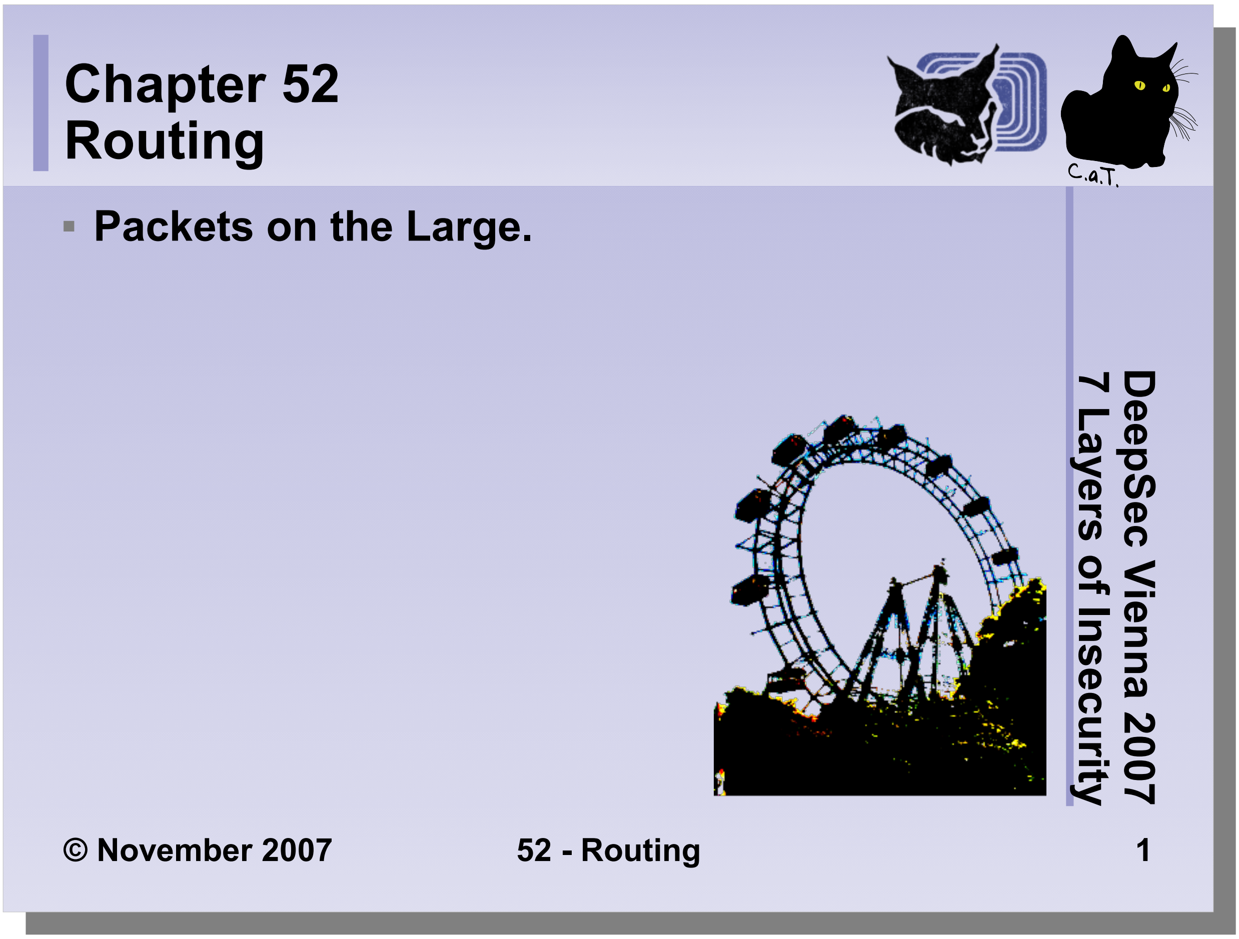
- Summary
  - Routing protocols can be attacked
  - Use authenticated updates
  - Use ingres filtering and anti spoofing

Thank You

C.a.T.

- **Questions?**

DeepSec Vienna 2007
7 Layers of Insecurity



Chapter 52
Routing

C.a.T.

- Packets on the Large.

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 52 - Routing 1

Copyright Information

C.a.T.

- Some rights reserved / Einige Rechte vorbehalten
- Michael Kafka, René Pfeiffer, Sebastian Meier
  C.a.T. Consulting and Trainings, Vienna, Austria
- You may freely use, distribute and modify this work under following agreement:
- Diese Arbeit darf frei genutzt, verbreitet und bearbeitet werden unter folgenden Bedingungen:

Authors must be referenced (also for modification)
Autoren müssen genannt werden (auch bei Bearbeitung)

Only for non commercial use
Nur für nichtkommerzielle Nutzung

Derivative work under same licence
Derivative Arbeit unter selber Lizenz

creative commons http://www.creativecommons.com

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 52 - Routing 2

This presentation is published under the CreativeCommons License which can be viewed in detail on their hompage: http://creativecommons.org/licenses/by-nc-sa/2.0/at/

Read more on http://www.creativecommons.com

You are free:

to Share — to copy, distribute and transmit the work

to Remix — to adapt the work

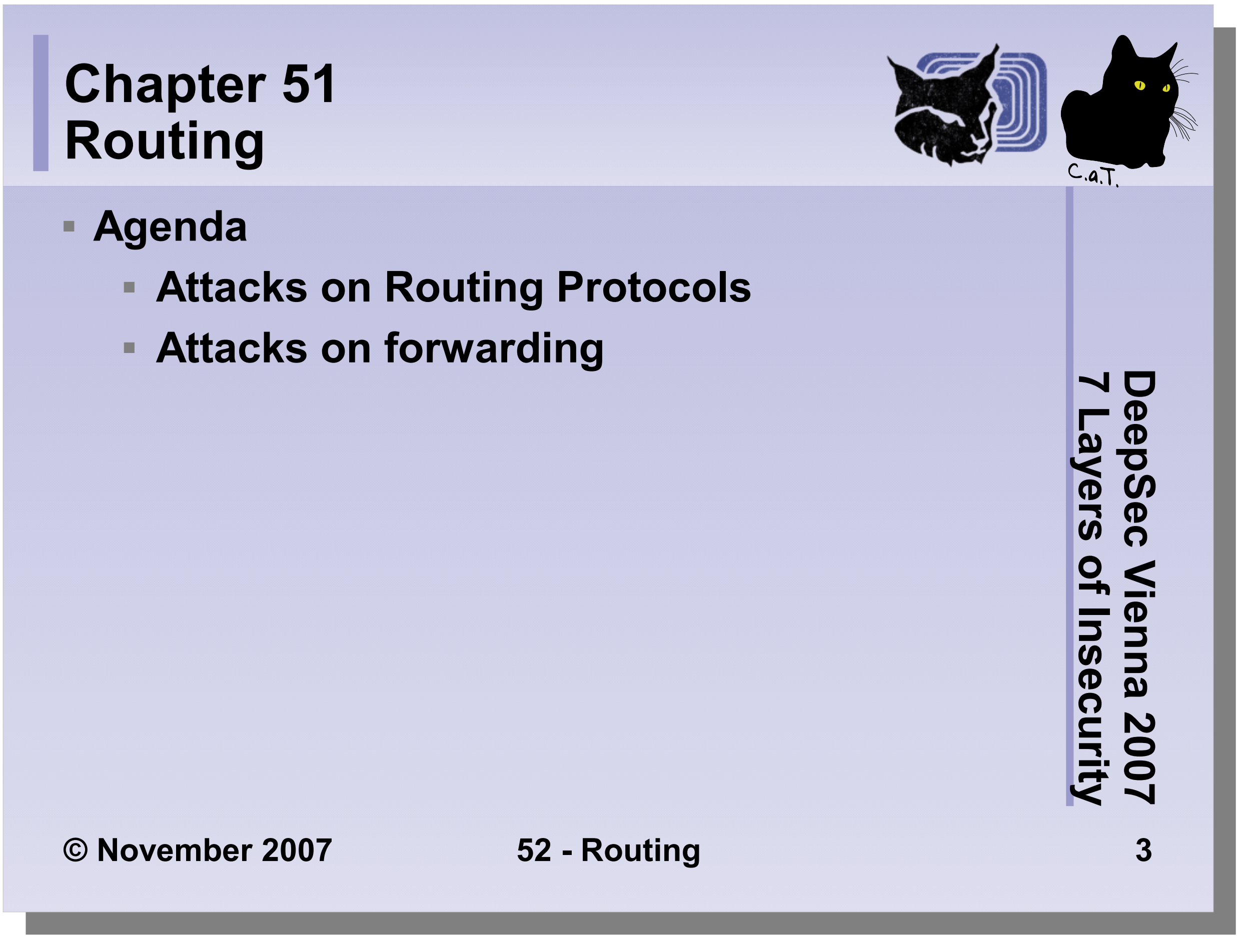
Under the following conditions:

Attribution. You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).

Noncommercial. You may not use this work for commercial purposes.

Share Alike. If you alter, transform, or build upon this work, you may distribute the resulting work only under the same or similar license to this one.

- For any reuse or distribution, you must make clear to others the license terms of this work. The best way to do this is with a link to this web page.
- Any of the above conditions can be waived if you get permission from the copyright holder.
- Nothing in this license impairs or restricts the author's moral rights.

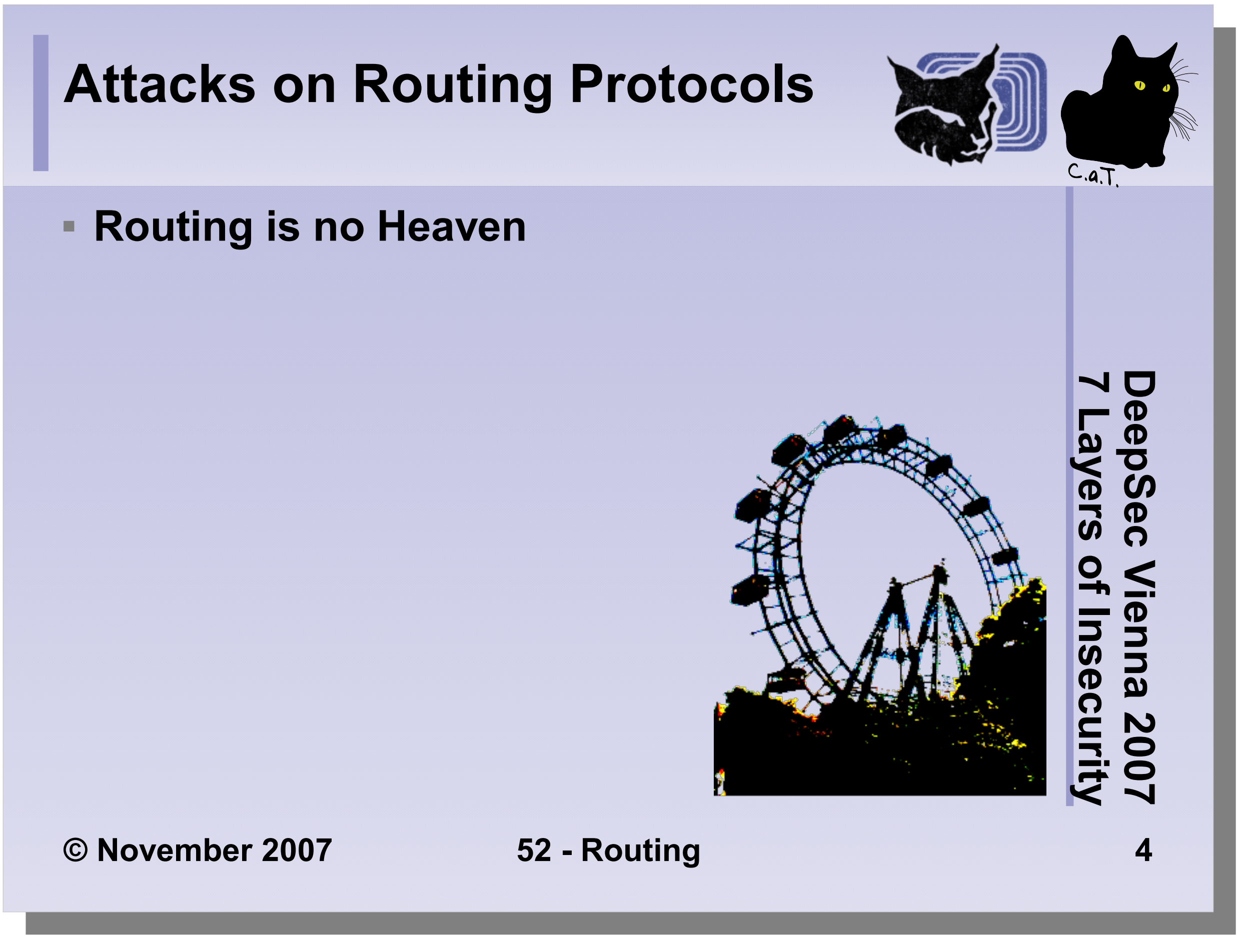


Chapter 51
Routing

- Agenda
  - Attacks on Routing Protocols
  - Attacks on forwarding

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 52 - Routing 3

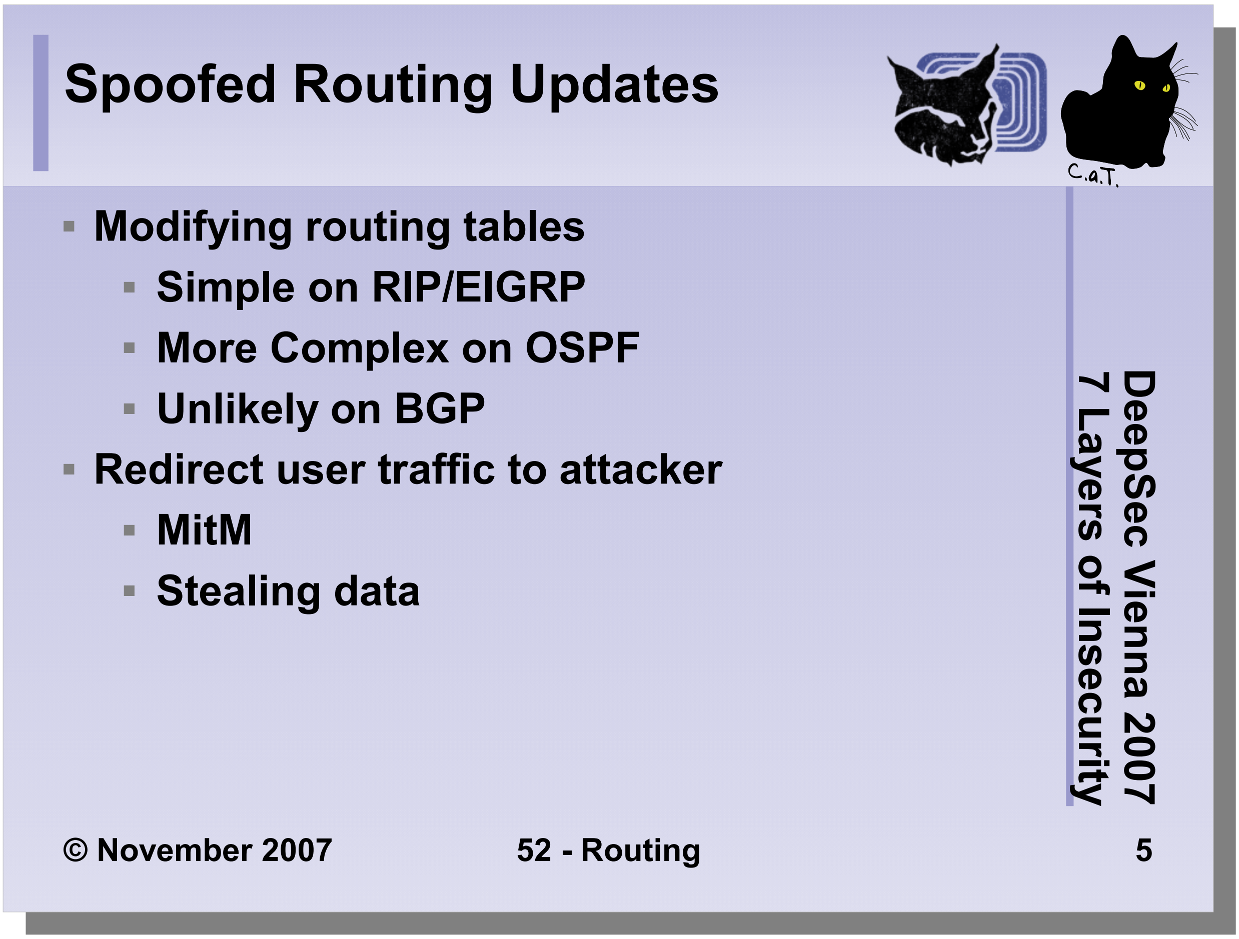


Attacks on Routing Protocols

- Routing is no Heaven

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 52 - Routing 4

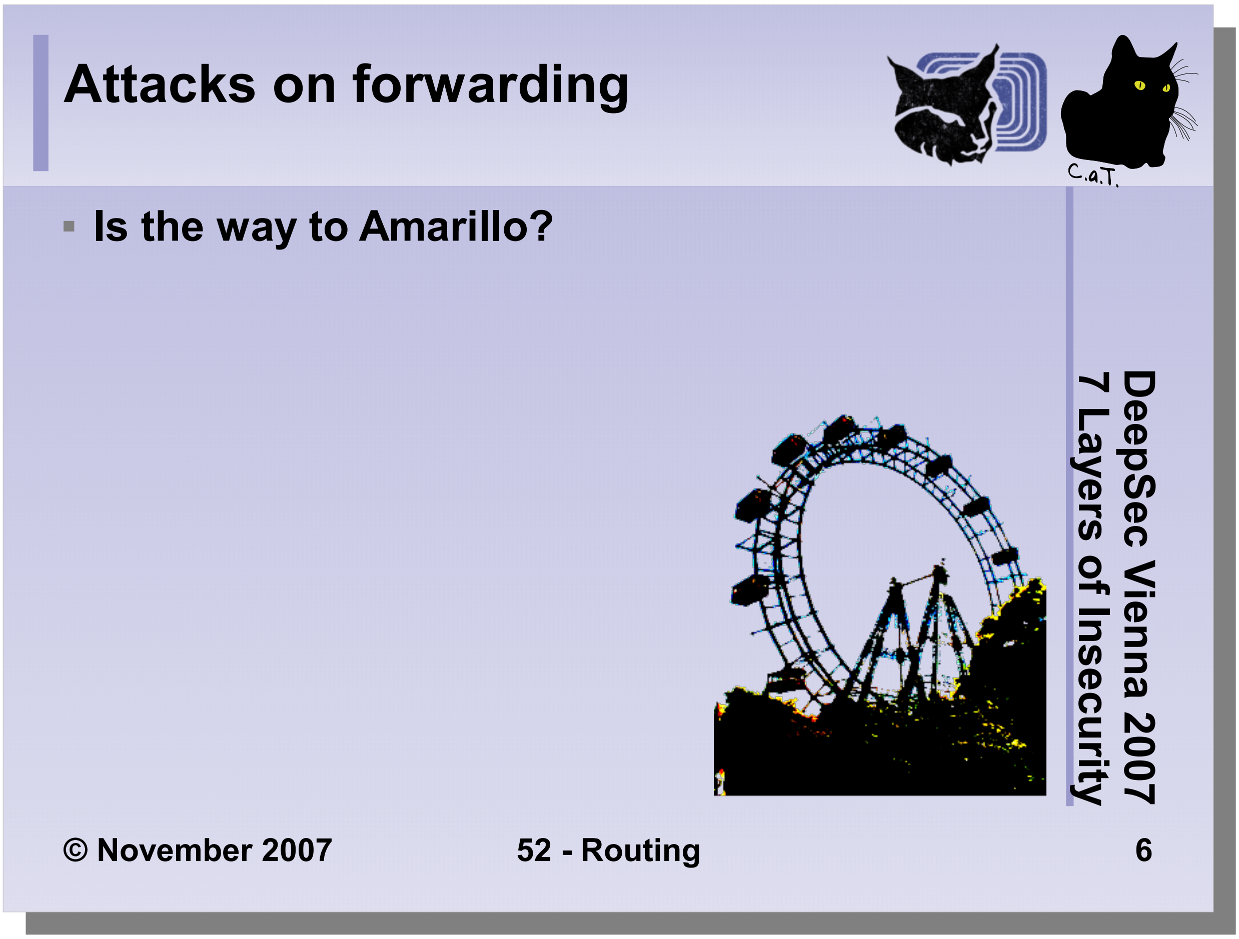


Spoofed Routing Updates

- Modifying routing tables
  - Simple on RIP/EIGRP
  - More Complex on OSPF
  - Unlikely on BGP
- Redirect user traffic to attacker
  - MitM
  - Stealing data

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 52 - Routing 5

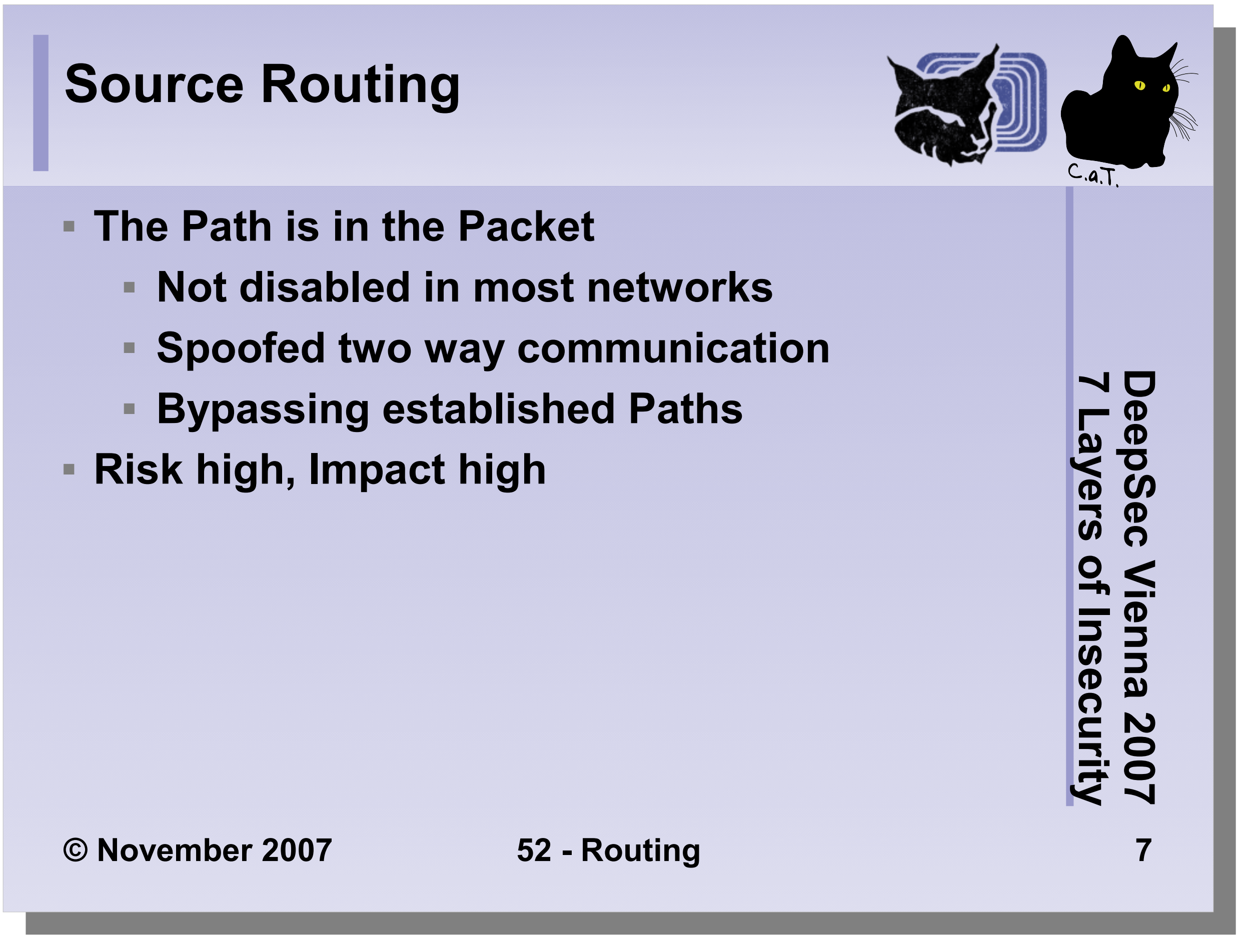


Attacks on forwarding

- Is the way to Amarillo?

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 52 - Routing 6

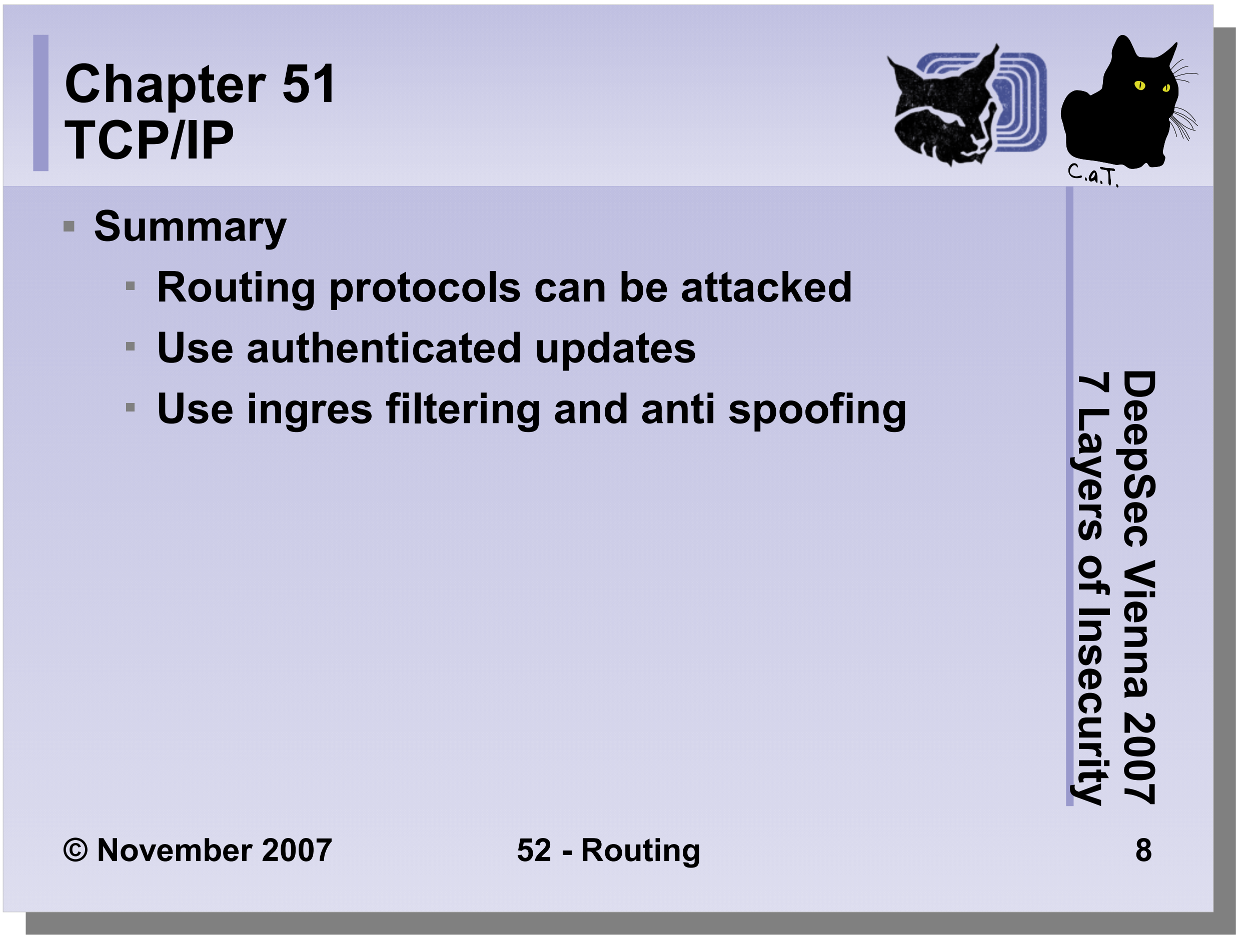


Source Routing

- The Path is in the Packet
  - Not disabled in most networks
  - Spoofed two way communication
  - Bypassing established Paths
- Risk high, Impact high

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 52 - Routing 7

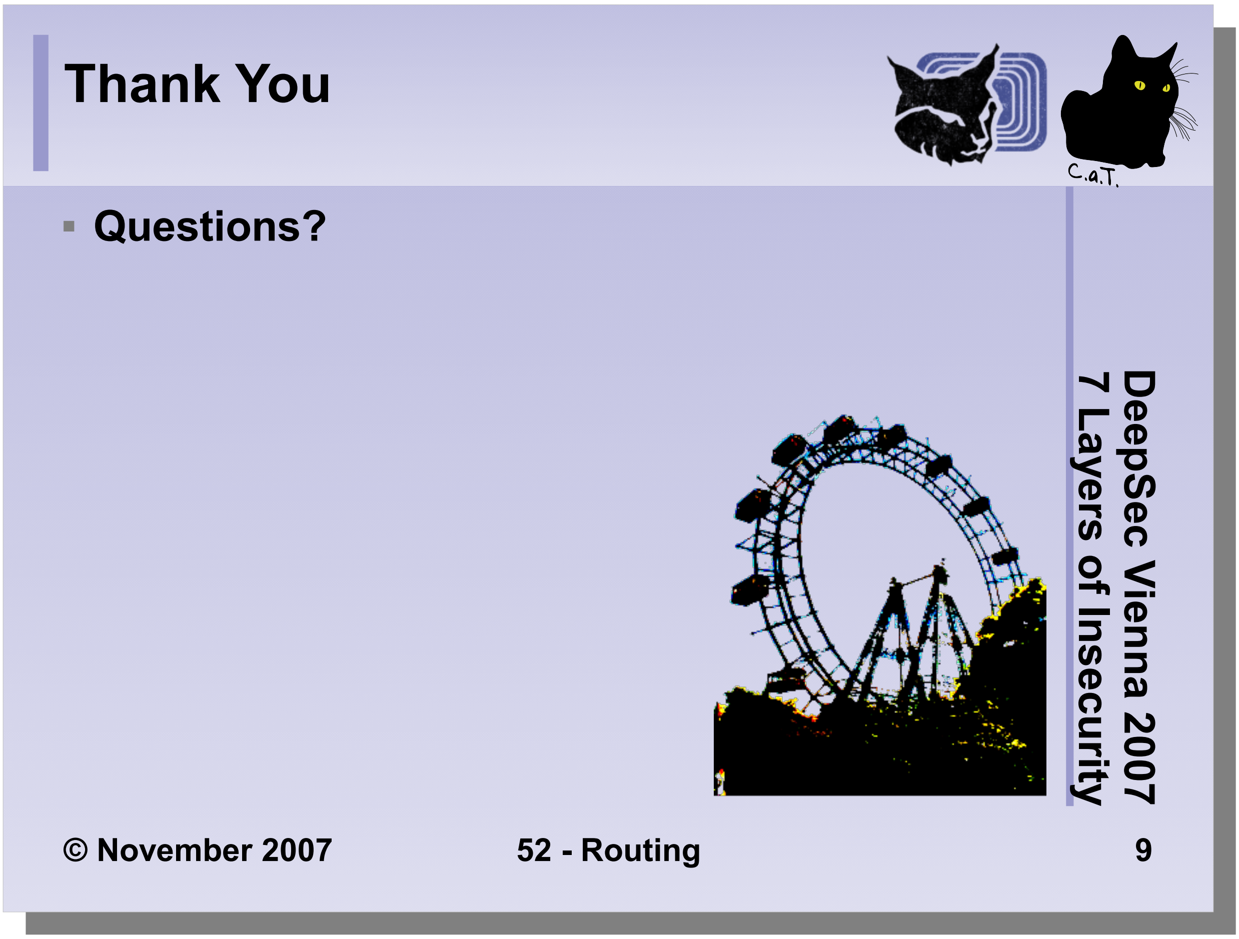


Chapter 51
TCP/IP

- Summary
  - Routing protocols can be attacked
  - Use authenticated updates
  - Use ingres filtering and anti spoofing

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 52 - Routing 8



Thank You

- Questions?

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 52 - Routing 9