Chapter 62
Simple Mail Transfer Protocol

- **You've got Mail!**

> **“President Bush said for security reasons, he's sworn off all e-mail communication. He will not be using email at the White House at all. Is that a good idea? I mean, it's not like that speaking thing was working out so good.”**

-- Jay Leno

DeepSec Vienna 2007
7 Layers of Insecurity

Copyright Information

- 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

© November 2007

Chapter 62
Simple Mail Transfer Protocol

- Agenda
  - SMTP Basics
  - SMTP Security Risks
  - Anti-Spam Frameworks
  - E-Mail Content

SMTP Basics

- The Foundation of Mail Delivery.

SMTP Properties

- Text based protocol
  - Commands use 7-bit ASCII
  - Data may use 8-bit encodings
- Message transmission as header+body
- Uses different TCP ports
  - 25/TCP for server-server communication
  - 465/TCP for SMTP+SSL
  - 587/TCP for message submission

DeepSec Vienna 2007
7 Layers of Insecurity

Sample SMTP Session

```
220 agamemnon.example.net ESMTP Postfix (Debian/GNU)
EHLO agamemnon.example.net
250-agamemnon.example.net
250-PIPELINING
250-SIZE 52428800
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
MAIL From: <lynx@example.net>
250 2.1.0 Ok
RCPT To: <lynx@agamemnon.example.net>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Hi!

Bye,
Lynx.
.
250 2.0.0 Ok: queued as 2CB7C24008A9
QUIT
221 2.0.0 Bye
```

Extended SMTP (ESMTP)

- Adds commands and functionalities
  - Command pipelining
  - SSL/TLS support
  - 8-bit support for data
  - On-demand relay for mobile users
- Many MTAs support ESMTP

SMTP Security Risks

- Let's Shoot the Messenger.

Open / Unauthorised Relays

- UBE/UCE still a big problem
  - Malware packed into email
  - Spam
- MTA needs to verify source of email
- *Any* open relay will be misused
  - Disrupt email delivery
  - Put IP range(s) on RBLs
- Risk: medium
- Impact: high

SMTP EHLO/HELO Pipe Bombs

- Imagine you inspect HELO strings
- Your logs look like this someday
  - 2007-…rblsmtp: 43 EHLO “|http://a.b.cc/cgi/put.cgi”
  - 2007-…rblsmtp: 43 HELO “|http://a.b.cc/cgi/put.cgi”
- Scripting security also applies to MTAs!
- Risk: medium
- Impact: high

SMTP VRFY

- SMTP VRFY tests email addresses
  - Existing accounts will be confirmed
  - (Ab)use for reconnaissance
- Some clients require VRFY
- MTAs may allow VRFY without announcement
- Risk: medium
- Impact: medium

DeepSec Vienna 2007
7 Layers of Insecurity

SMTP Authentication

- Protocol offers no authentication
  - Sender/recipient is arbitrary
  - Mail relaying must be tightly controlled
- MITM attacks can be easily done
- Spoofing of messages very easy

DeepSec Vienna 2007
7 Layers of Insecurity

SMTP AUTH

- ESMTP offers authentication
  - Used for MUA→MTA / MTA→MTA
  - Email addresses stay unauthenticated
- Reduces open relay problem
  - Lost/brute-forced password critical
- Useful for mobile users
- Most MTA support SASL mechanisms

SMTP + SSL/TLS

- Works with keys & certificates
  - Provides everything that SSL/TLS promises
- MTAs usually have no trust relationship
  - Self-signed certificates
  - Certificates are next to never verified
  - MITM still possible
- Risk: medium
- Impact: medium

DeepSec Vienna 2007
7 Layers of Insecurity

Anti-Spam Frameworks

- Enhanced Complexity as Security Measure.

Domain Keys

- Adds header with signature
  - Signed content of message
  - Signature linked to domain name
- Cryptographic checksums per message
- In-transit modification breaks checks
  - Mailing list managers
  - Content filter
- Envelope not part of signature
  - Replay injection possible

Domain Keys & DNS

- DomainKey-Signature header has fields: …d=example.net; s=dkim.key;…
- PK lookup: dkim.key._domainkey.example.net
- DNS security determines DKIM security
  - DNS attacks apply as well
  - Attacker may try to offer own key

DeepSec Vienna 2007
7 Layers of Insecurity

Sender Policy Framework (SPF)

- Based on published policies in DNS
  - Domains name valid email origins
  - Domains name default trust level
- SPF works in SMTP dialogue
  - Early blocking possible
- SPF *completely* breaks email forwarding
  - Message must be rewritten
  - Sender Rewriting Scheme (SRS)

Real Time Blacklisting (RBL)

- RBL are simply based on lists
  - Distribution by DNS is common
  - Listing may have arbitrary parameters
- Most RBLs are based on reputation
  - Metrics help measurement
  - Scores can change dynamically
- Using any RBL outsources access lists

DeepSec Vienna 2007
7 Layers of Insecurity

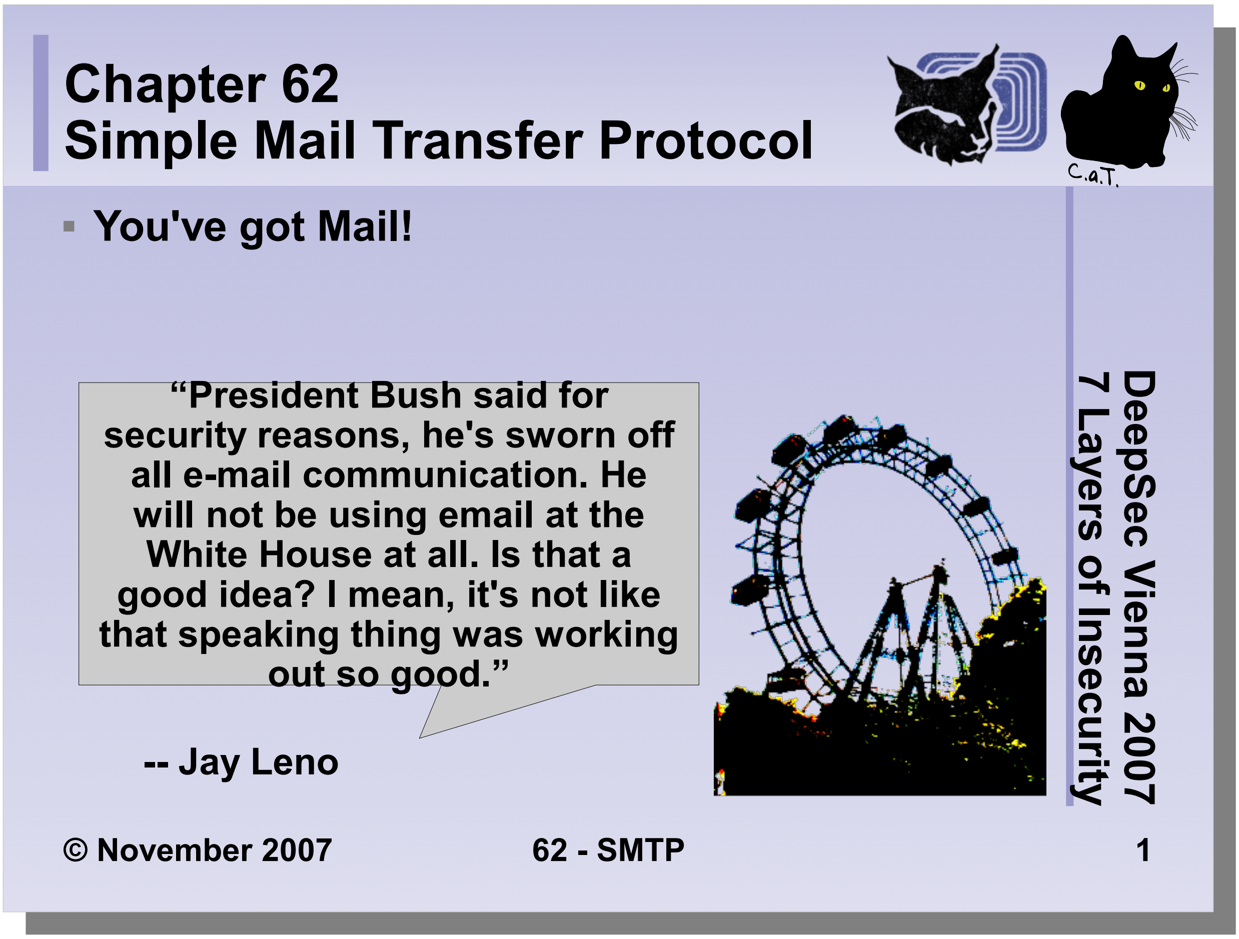
Chapter 62
Simple Mail Transfer Protocol

- Summary
  - SMTP needs protection.
  - SMTP relies on DNS infrastructure.
  - SMTP + SSL/TLS isn't necessarily safe.
  - SMTP servers on RBL are useless.
  - Pick RBLs carefully.

Thank You

- Questions?

DeepSec Vienna 2007
7 Layers of Insecurity



Chapter 62
Simple Mail Transfer Protocol

- You've got Mail!

> “President Bush said for security reasons, he's sworn off all e-mail communication. He will not be using email at the White House at all. Is that a good idea? I mean, it's not like that speaking thing was working out so good.”

-- Jay Leno

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 62 - SMTP 1

Copyright Information

- 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 62 - SMTP 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

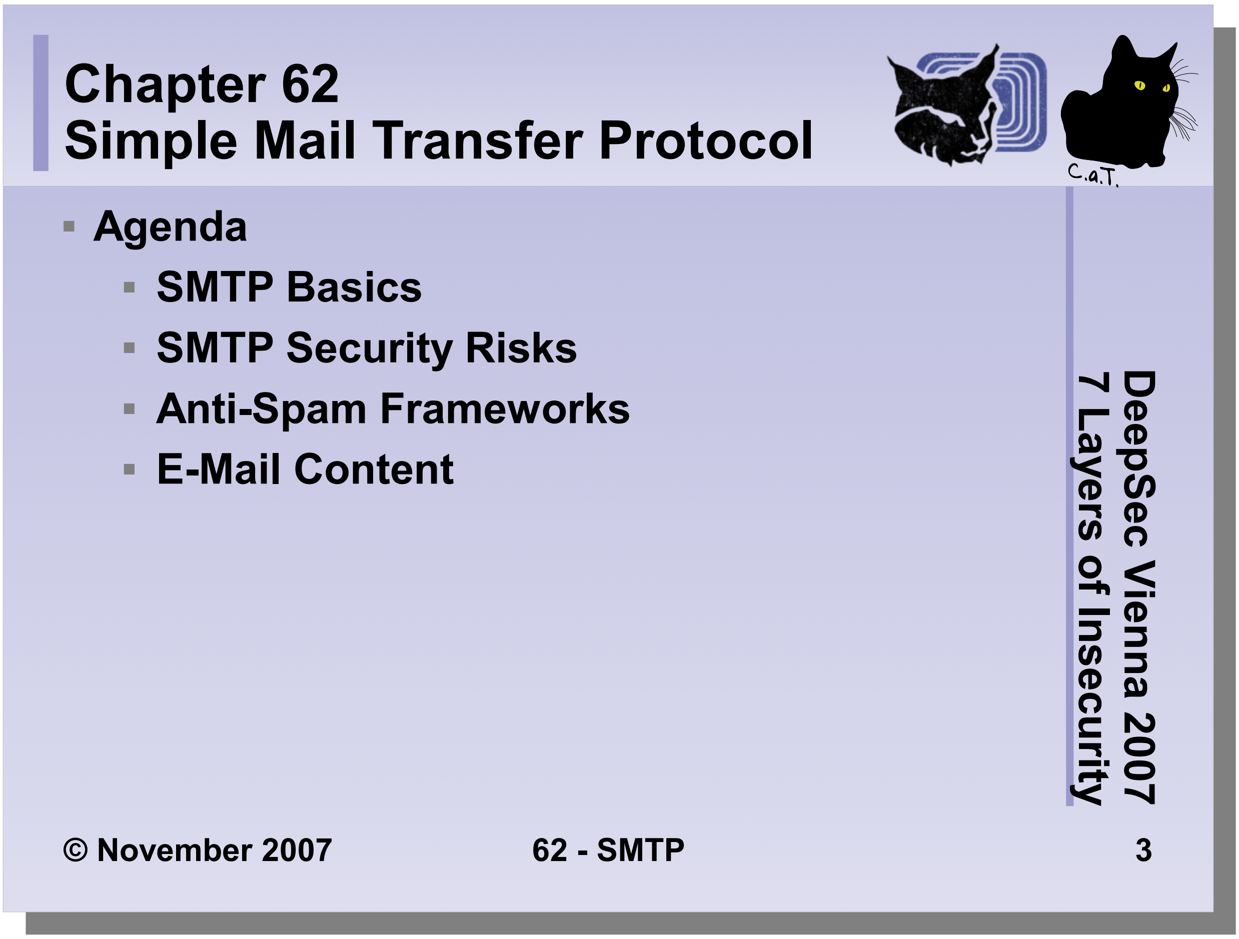
Under the following conditions:

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.

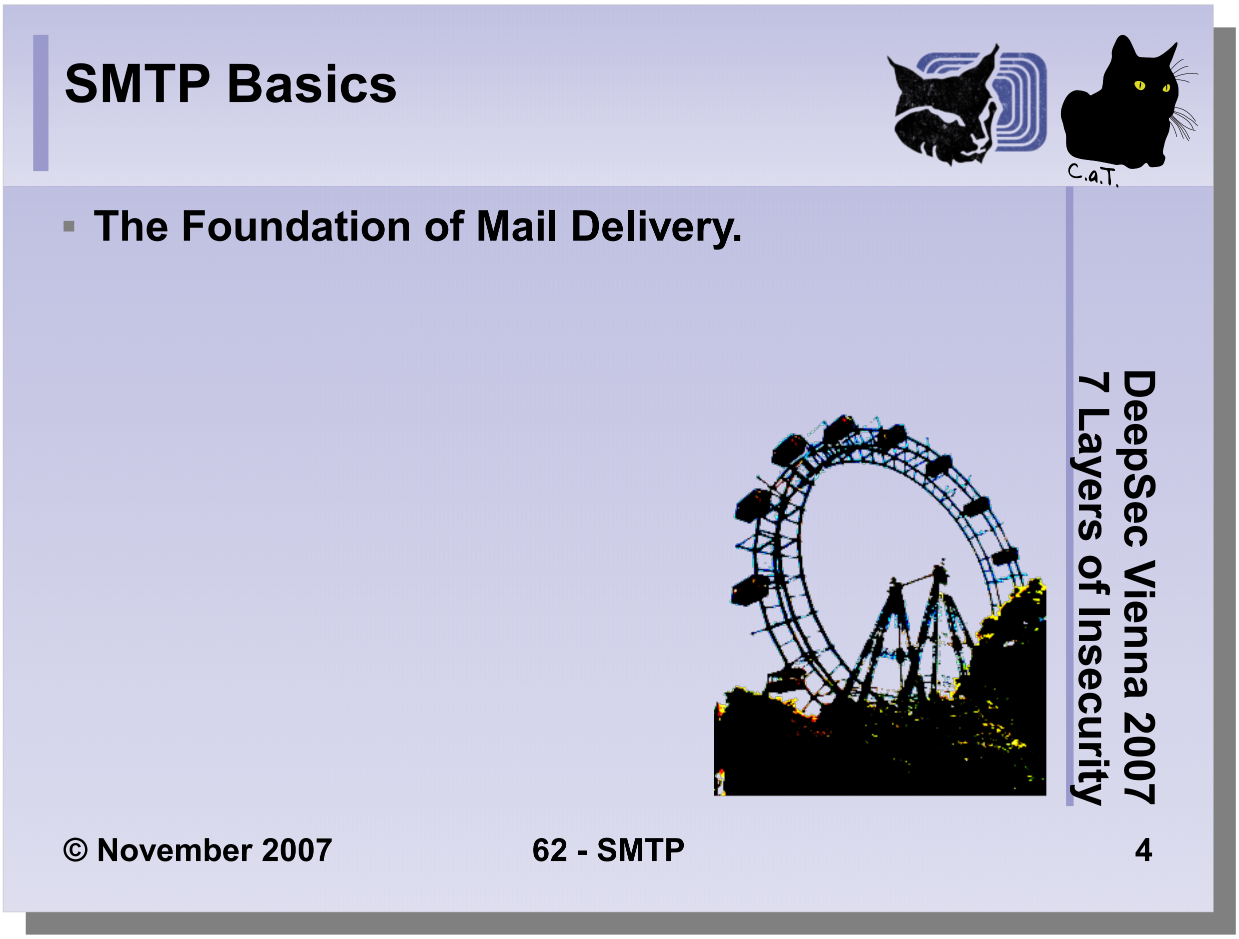


Chapter 62
Simple Mail Transfer Protocol

- Agenda
  - SMTP Basics
  - SMTP Security Risks
  - Anti-Spam Frameworks
  - E-Mail Content

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 62 - SMTP 3

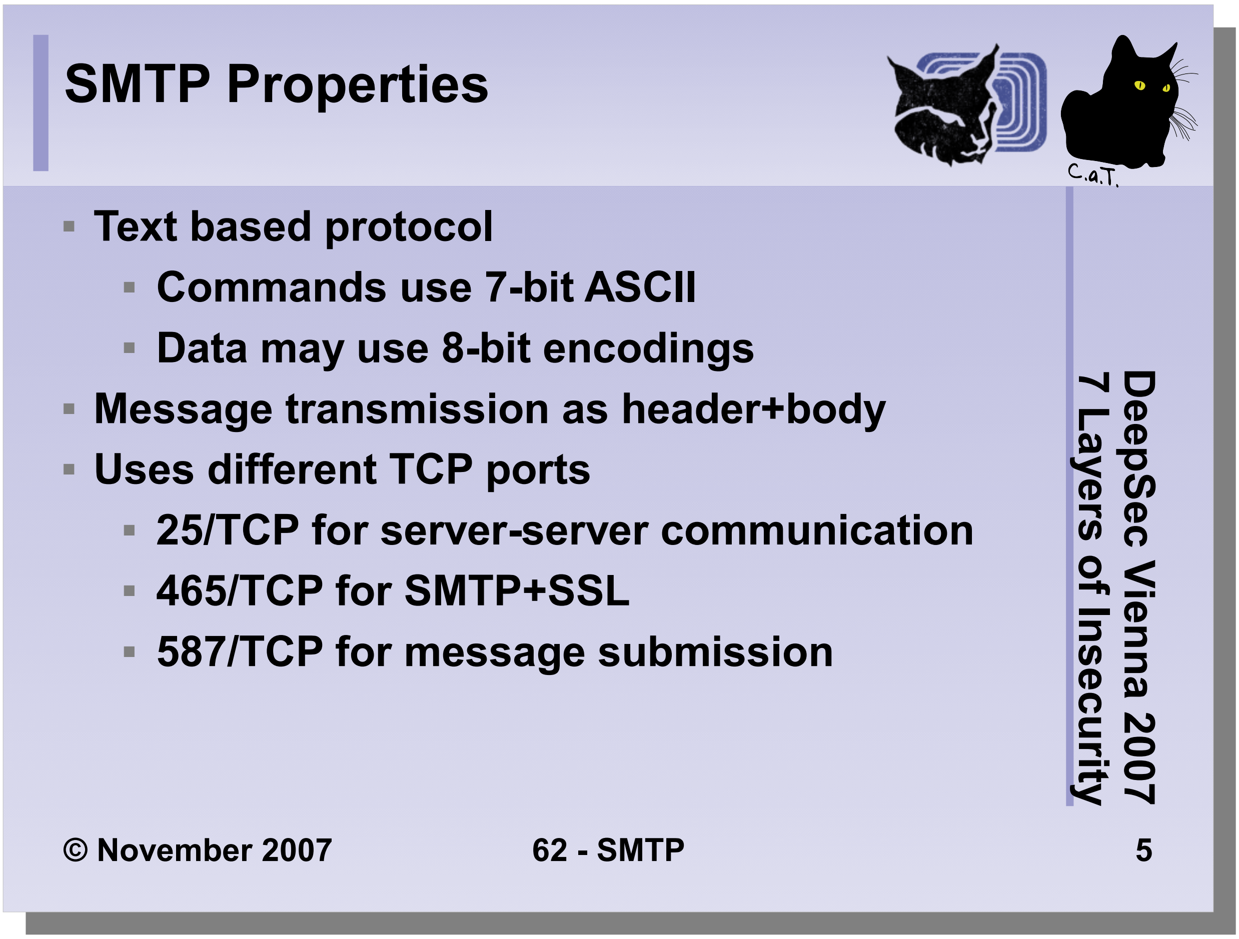


SMTP Basics

- The Foundation of Mail Delivery.

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 62 - SMTP 4



SMTP Properties

C.a.T.

- Text based protocol
  - Commands use 7-bit ASCII
  - Data may use 8-bit encodings
- Message transmission as header+body
- Uses different TCP ports
  - 25/TCP for server-server communication
  - 465/TCP for SMTP+SSL
  - 587/TCP for message submission

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 62 - SMTP 5

SMTP/ESMTP transactions distinguish between three roles of the endpoint.

• Mail Submission Agent (MSA) receives email from a MUA and relays it to other MTAs.

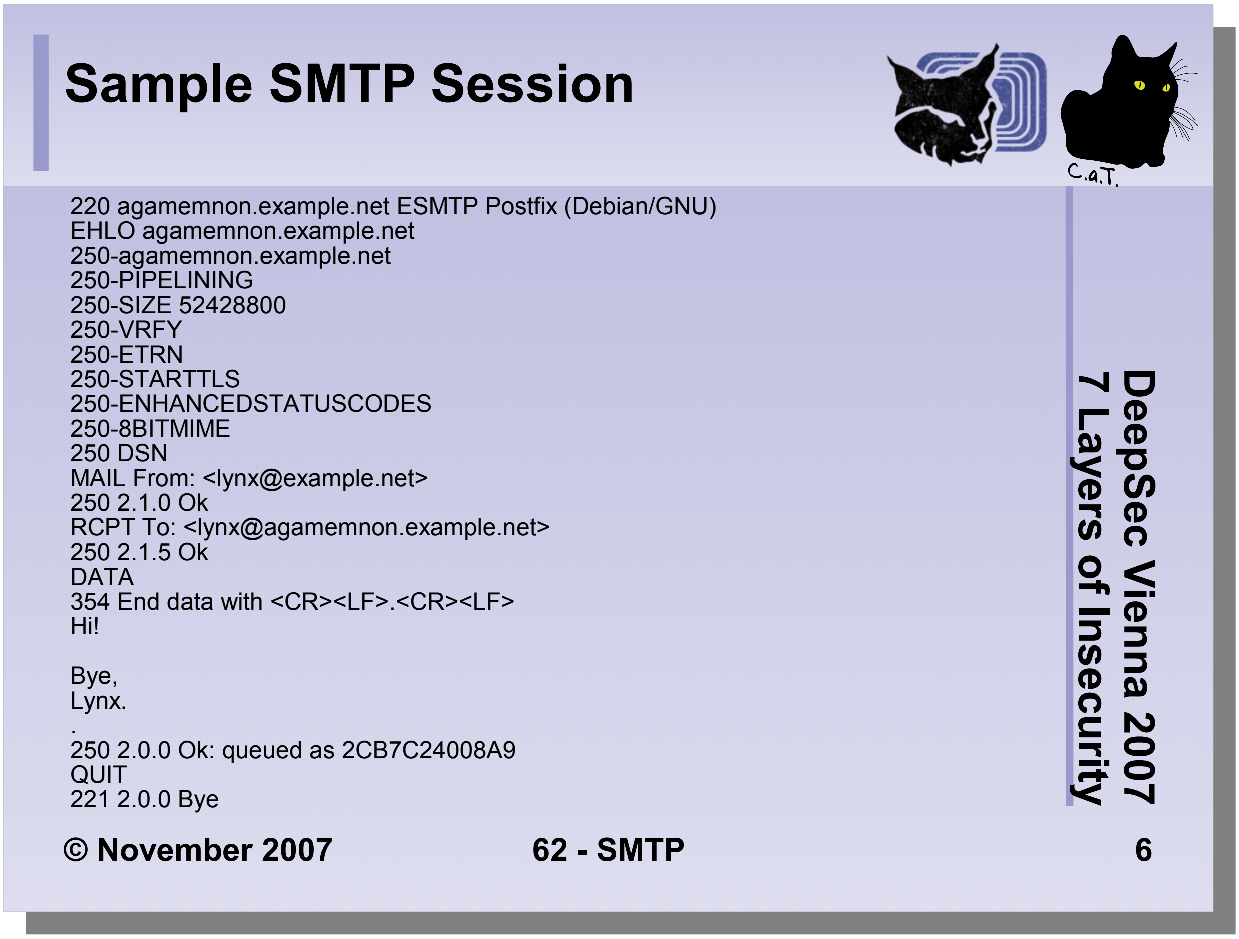
• Mail Transport Agent (MTA) is the classical “mail server” that transports email messages to other MTAs.

• Mail User Agent (MUA) is the classical “mail software” that enables users to read, write and send email.

MTAs speak ESMTP/SMTP with each other on port 25/TCP. MUAs submit their messages either via ESMTP/SMTP to a MTA on port 25/TCP or to a MSA on port 587/TCP. Submission by using MSA supports mobile users and offers authentication along with correction of the submitted messages (adding missing header fields for example). In practice most MUAs use a local MTA or submission via 25/TCP.

ESMTP/SMTP is proposed in RFC 821, 822, 2821, 2822 among others.

Message submission via 587/TCP is proposed in RFC 2476.



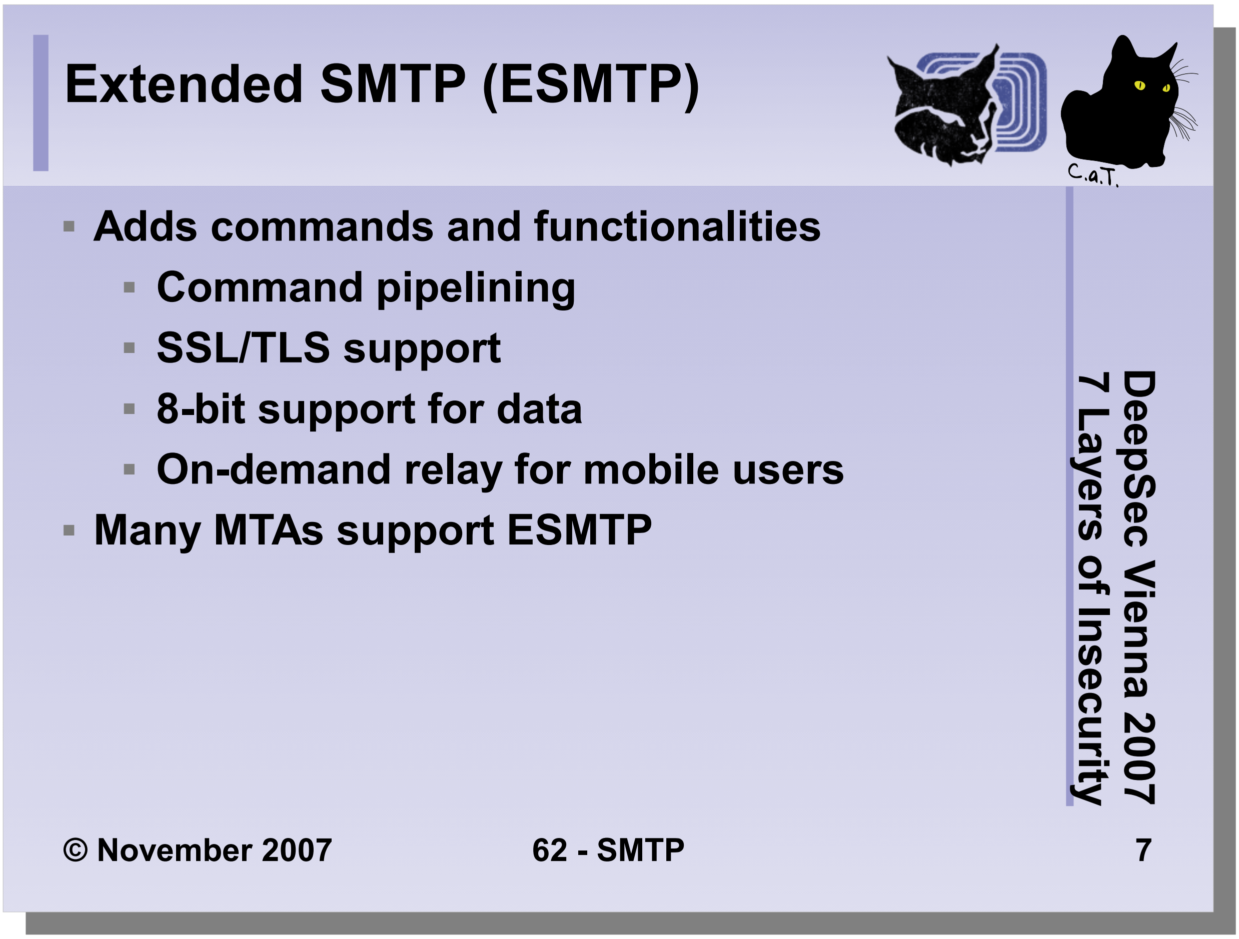
Sample SMTP Session

```
220 agamemnon.example.net ESMTP Postfix (Debian/GNU)
EHLO agamemnon.example.net
250-agamemnon.example.net
250-PIPELINING
250-SIZE 52428800
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
MAIL From: <lynx@example.net>
250 2.1.0 Ok
RCPT To: <lynx@agamemnon.example.net>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Hi!

Bye,
Lynx.
.
250 2.0.0 Ok: queued as 2CB7C24008A9
QUIT
221 2.0.0 Bye
```

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 62 - SMTP 6

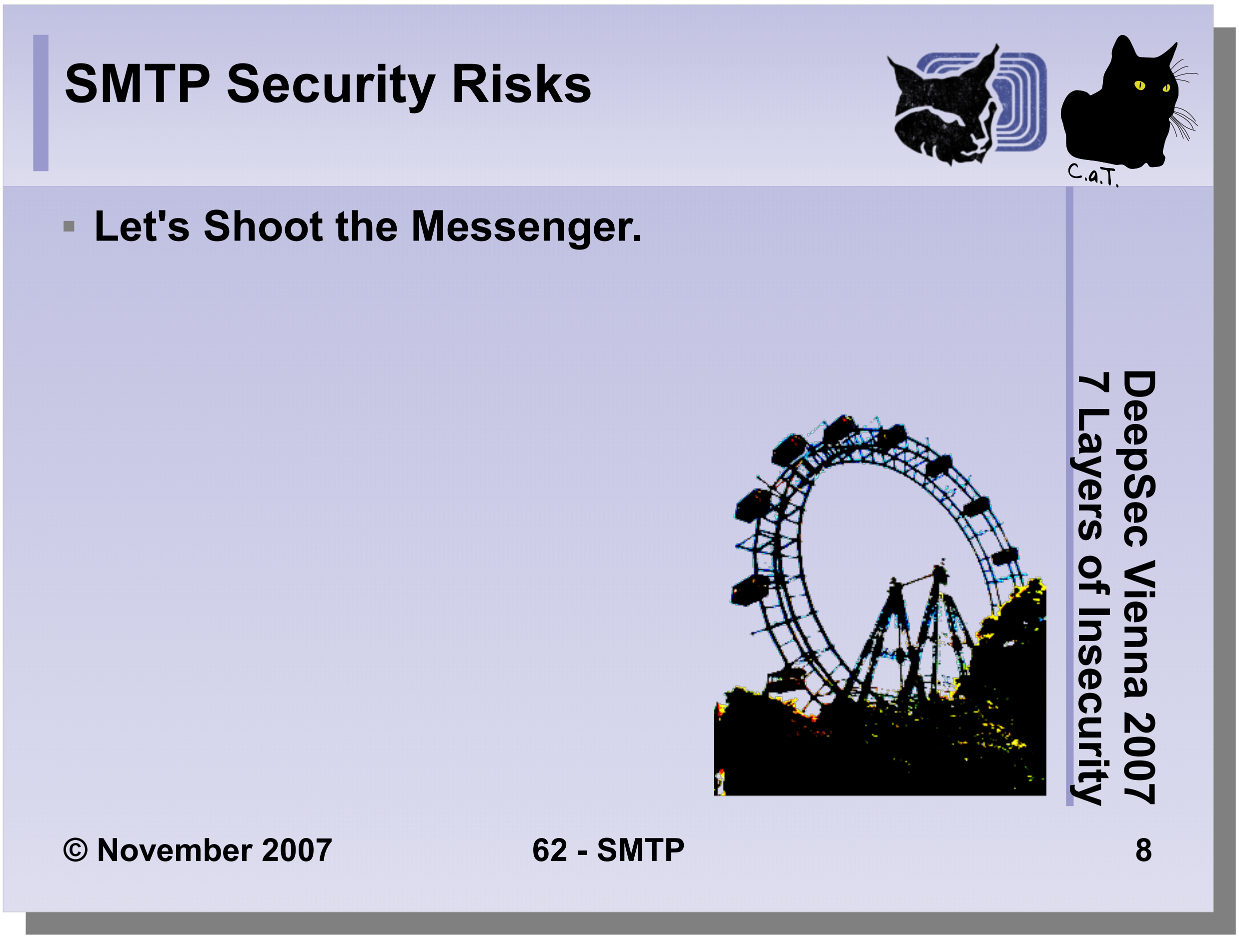


Extended SMTP (ESMTP)

- Adds commands and functionalities
  - Command pipelining
  - SSL/TLS support
  - 8-bit support for data
  - On-demand relay for mobile users
- Many MTAs support ESMTP

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 62 - SMTP 7

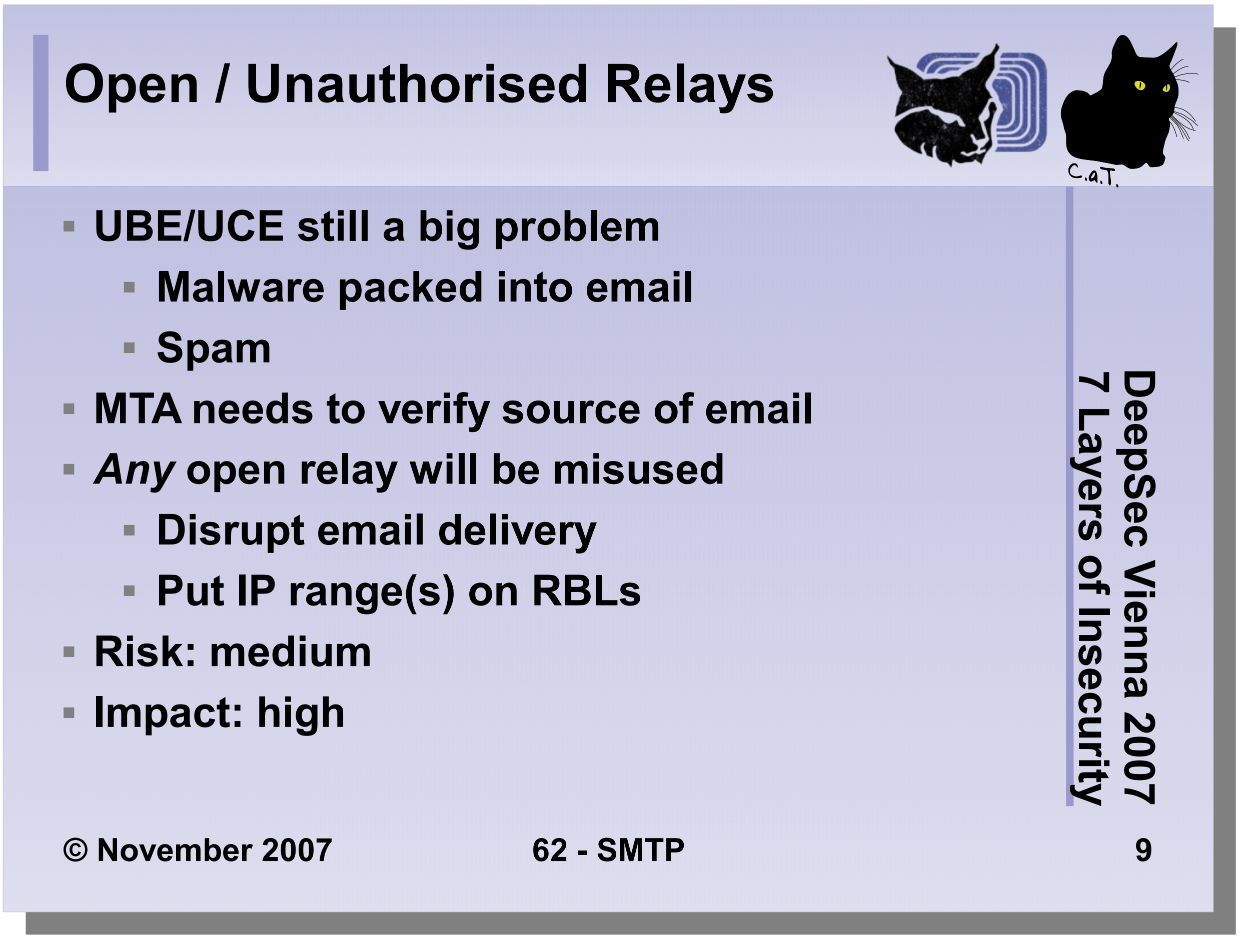


SMTP Security Risks

- Let's Shoot the Messenger.

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 62 - SMTP 8



Open / Unauthorised Relays

- UBE/UCE still a big problem
  - Malware packed into email
  - Spam
- MTA needs to verify source of email
- *Any* open relay will be misused
  - Disrupt email delivery
  - Put IP range(s) on RBLs
- Risk: medium
- Impact: high

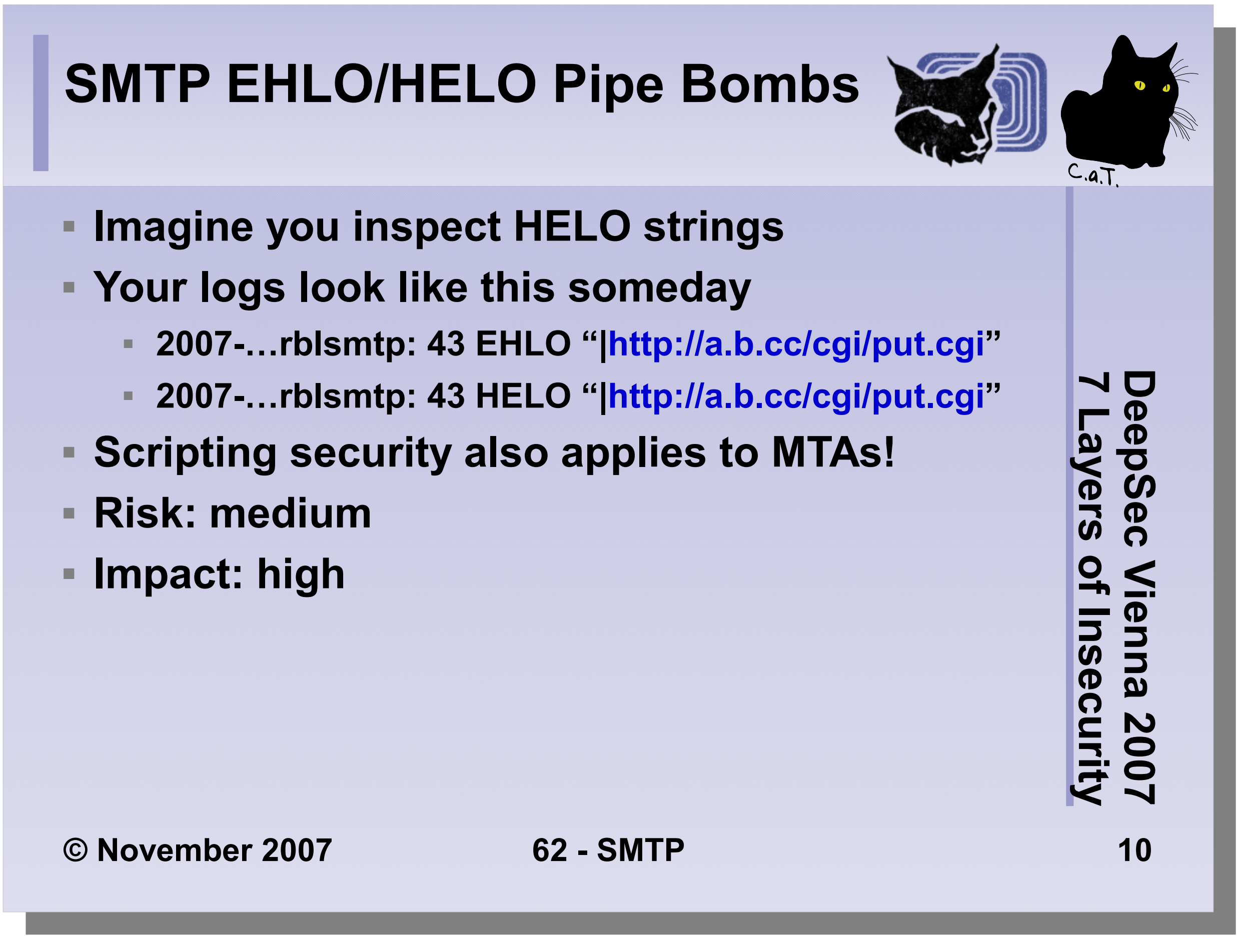
DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 62 - SMTP 9

Most MTAs are equipped with anti-spam and anti-virus filters. This is no safeguard against open relaying of malware or email messages. A lot of servers have satellite MTAs installed that act only as a collector for locally generated email. Usually the central mail hub gets all messages and delivers them. The mail filters are not equally strong and so a satellite MTA may inject malformed messages, thus discrediting the central MTA when the emails leave the network. ISPs often suffer from this effect, because they have to relay mail from their customers. The same can happen to a LAN where the outbound MTA trusts every client. DMZs usually have their share of web servers that might act as HTTP-to-SMTP gateway and also feed the central MTA with malware or spam emails.

Mitigation:

- Tightly configure access rules for *all* of your MTAs.
- Inspect internal email as you would inspect external email messages.
- Use multiple outbound relays and use them for specific classes of email.



SMTP EHLO/HELO Pipe Bombs

- Imagine you inspect HELO strings
- Your logs look like this someday
  - 2007-…rblsmtp: 43 EHLO "|http://a.b.cc/cgi/put.cgi"
  - 2007-…rblsmtp: 43 HELO "|http://a.b.cc/cgi/put.cgi"
- Scripting security also applies to MTAs!
- Risk: medium
- Impact: high

DeepSec Vienna 2007
7 Layers of Insecurity

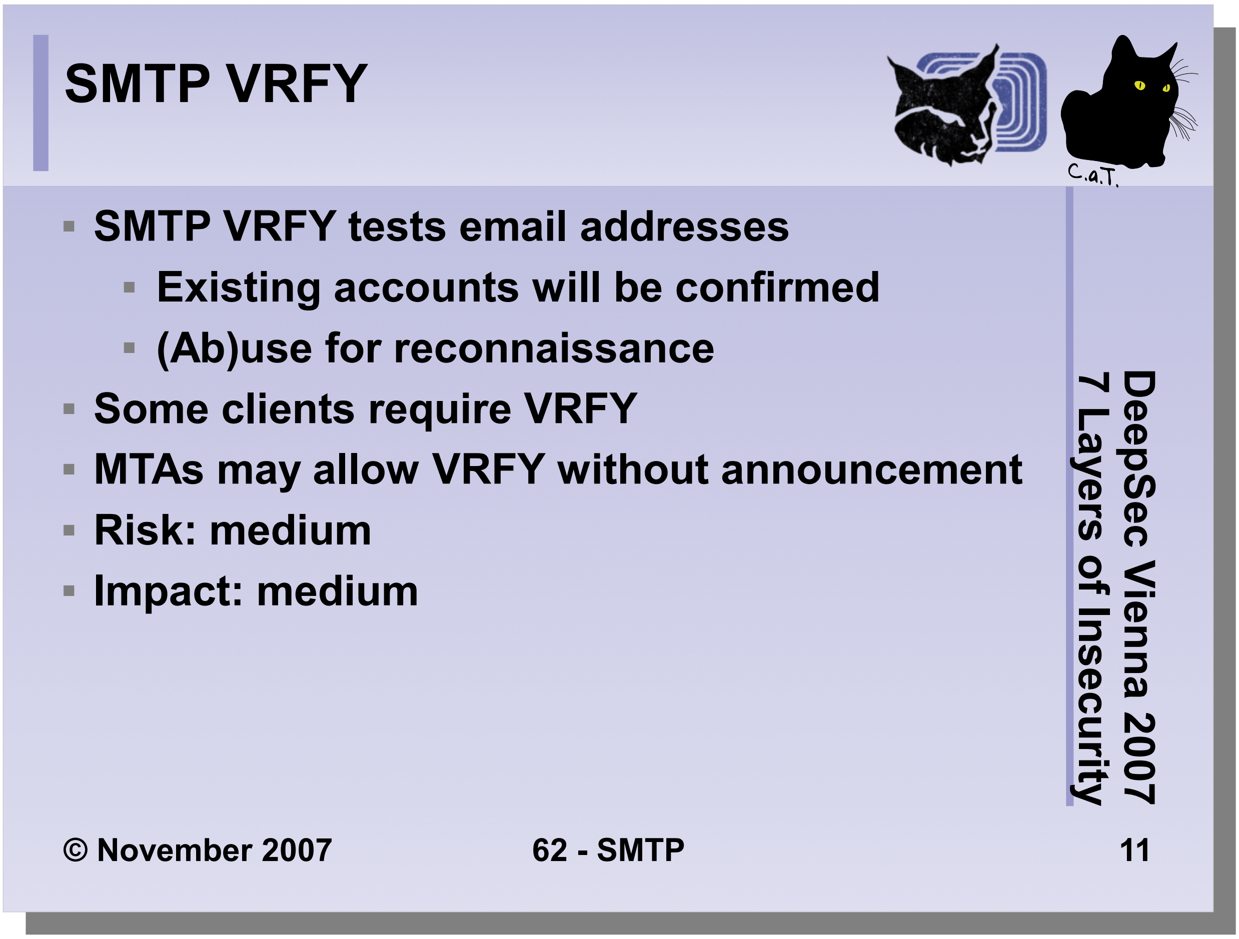
© November 2007 62 - SMTP 10

Mitigation:

• Be careful with MTA functionality augmented by plugins.

• Limit MTA software on server (access controls, privileges).

• Do security checks with all your filtering systems (collections of malformed email can be generated and are available).



SMTP VRFY

- SMTP VRFY tests email addresses
  - Existing accounts will be confirmed
  - (Ab)use for reconnaissance
- Some clients require VRFY
- MTAs may allow VRFY without announcement
- Risk: medium
- Impact: medium

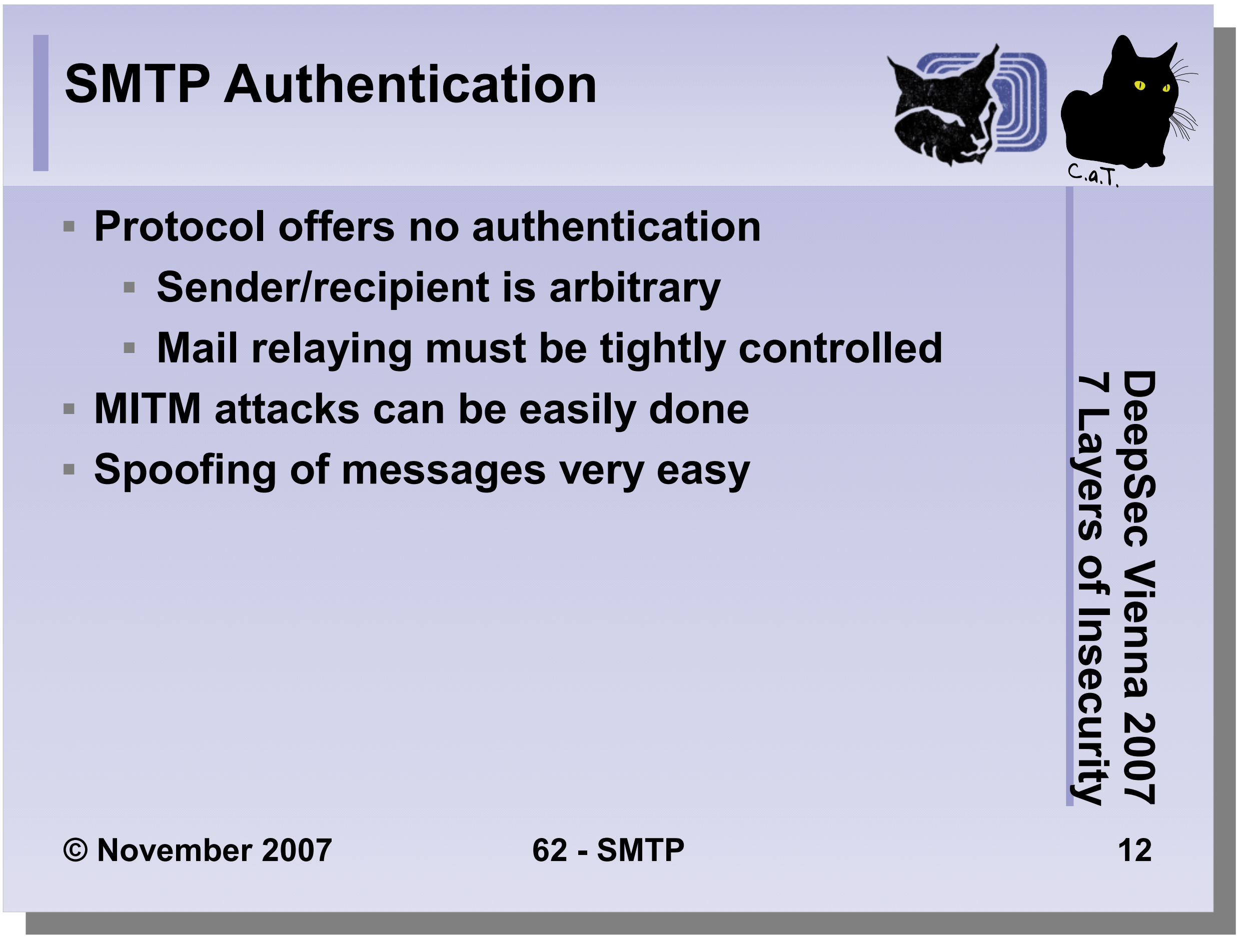
DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 62 - SMTP 11

Account/address enumeration is a tool routinely used by attackers. SMTP is one way of getting hold of verified information, harvesting LDAP trees is another.

Mitigation:

- Disable VRFY if possible.
- Disable the EXPN command (allows listing of mailing list subscribers).
- Limit SMTP connection and disconnect after *n* invalid commands or errors.
- Deploy SMTP greylisting and rate limiting at your border MTAs.

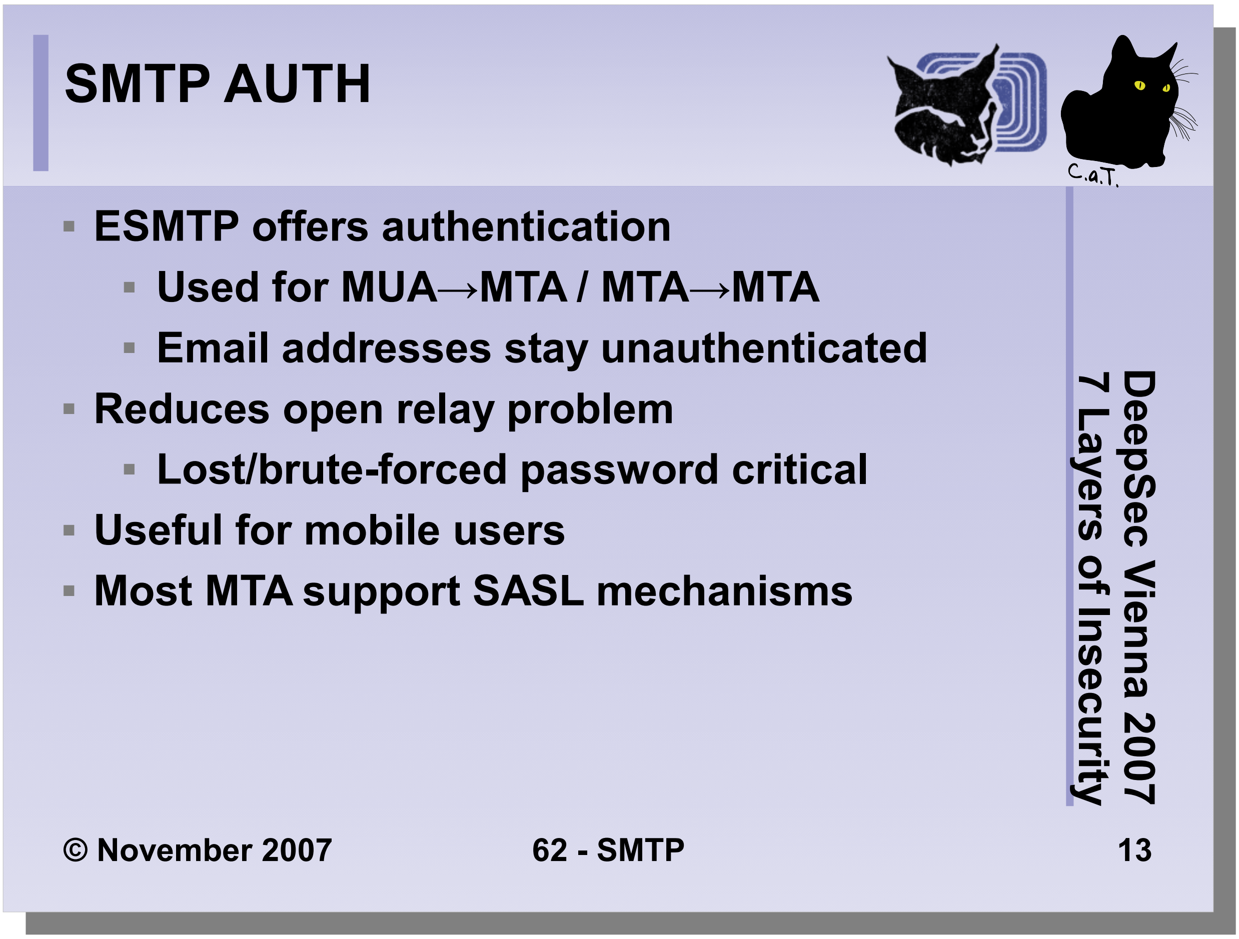


SMTP Authentication

- Protocol offers no authentication
  - Sender/recipient is arbitrary
  - Mail relaying must be tightly controlled
- MITM attacks can be easily done
- Spoofing of messages very easy

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 62 - SMTP 12

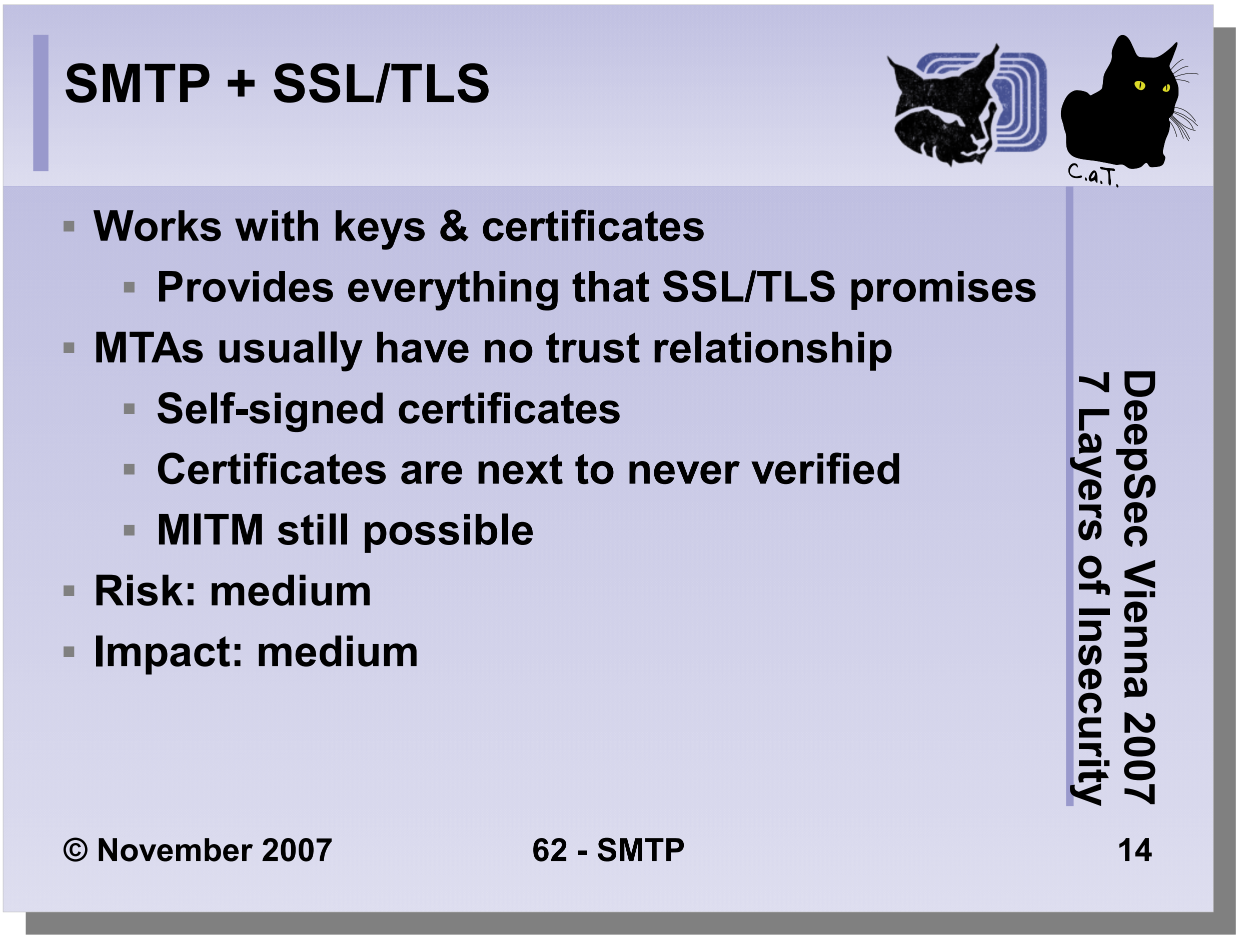


SMTP AUTH

- ESMTP offers authentication
  - Used for MUA→MTA / MTA→MTA
  - Email addresses stay unauthenticated
- Reduces open relay problem
  - Lost/brute-forced password critical
- Useful for mobile users
- Most MTA support SASL mechanisms

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 62 - SMTP 13



SMTP + SSL/TLS

C.a.T.

- Works with keys & certificates
  - Provides everything that SSL/TLS promises
- MTAs usually have no trust relationship
  - Self-signed certificates
  - Certificates are next to never verified
  - MITM still possible
- Risk: medium
- Impact: medium

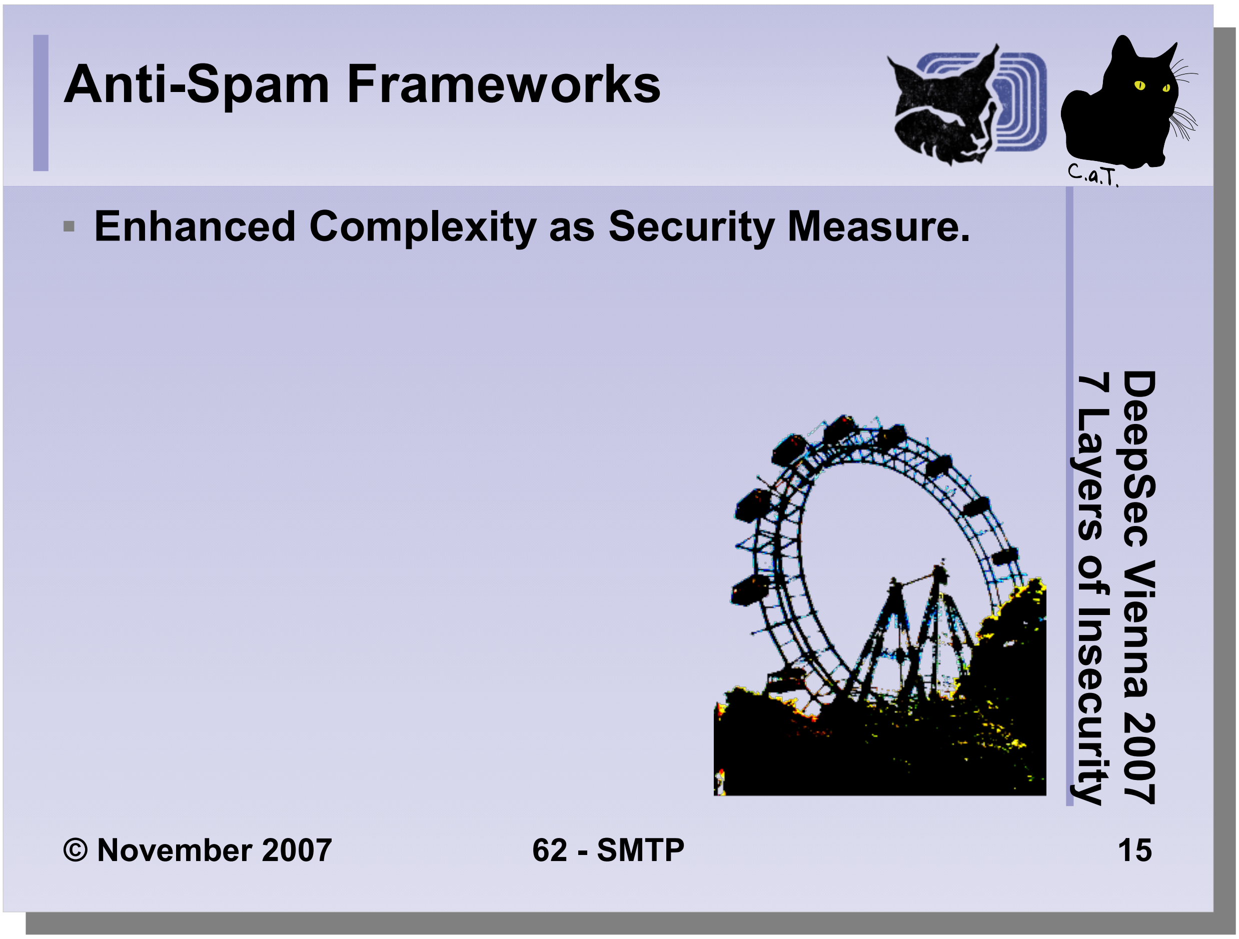
DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 62 - SMTP 14

Most MTAs can be configured to deny unencrypted SMTP sessions. However this breaks the SMTP specification and thus can only used for clients and networks under your control.

Mitigation:

- Use certificate verification on a dedicated TLS-only MTA for roaming users.
- Use VPN technology to bring roaming users to your MTA.

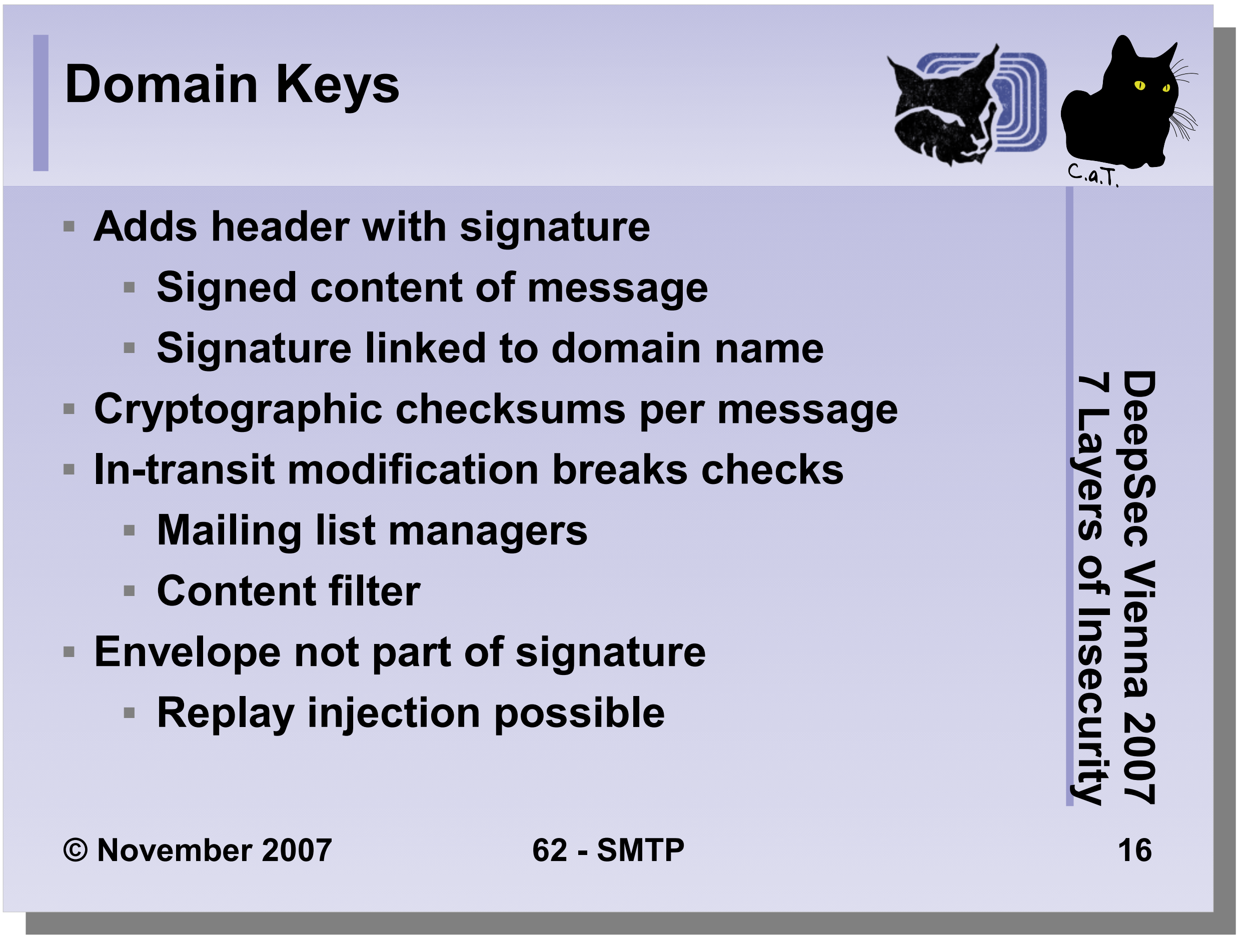


Anti-Spam Frameworks

- Enhanced Complexity as Security Measure.

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 62 - SMTP 15



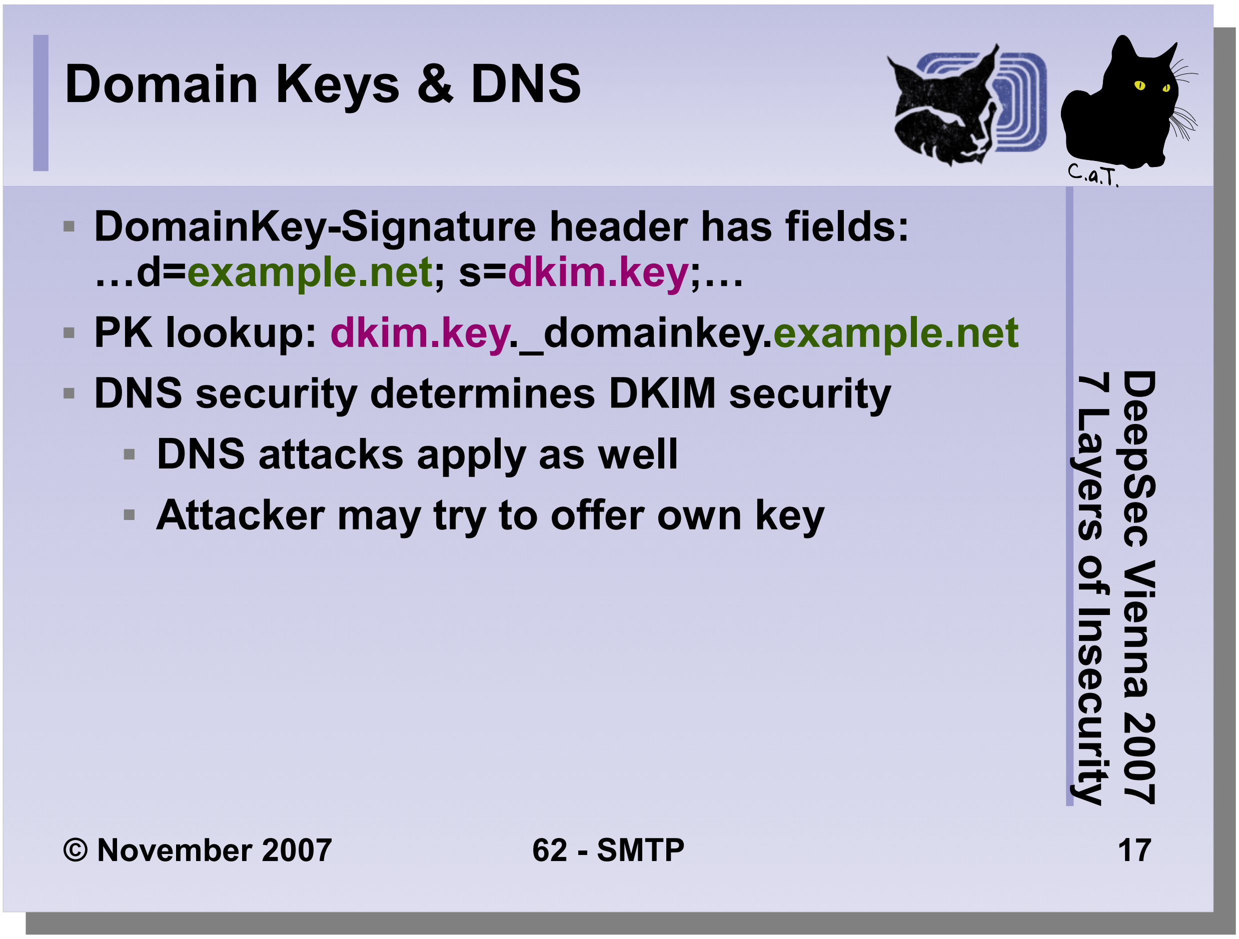
Domain Keys

- Adds header with signature
  - Signed content of message
  - Signature linked to domain name
- Cryptographic checksums per message
- In-transit modification breaks checks
  - Mailing list managers
  - Content filter
- Envelope not part of signature
  - Replay injection possible

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 62 - SMTP 16

Domain Keys should always be used as a component in a layered security design. Use it in combination with VPN technologies, SSL/TLS, authentication and verified configurations of MUAs/MTAs.

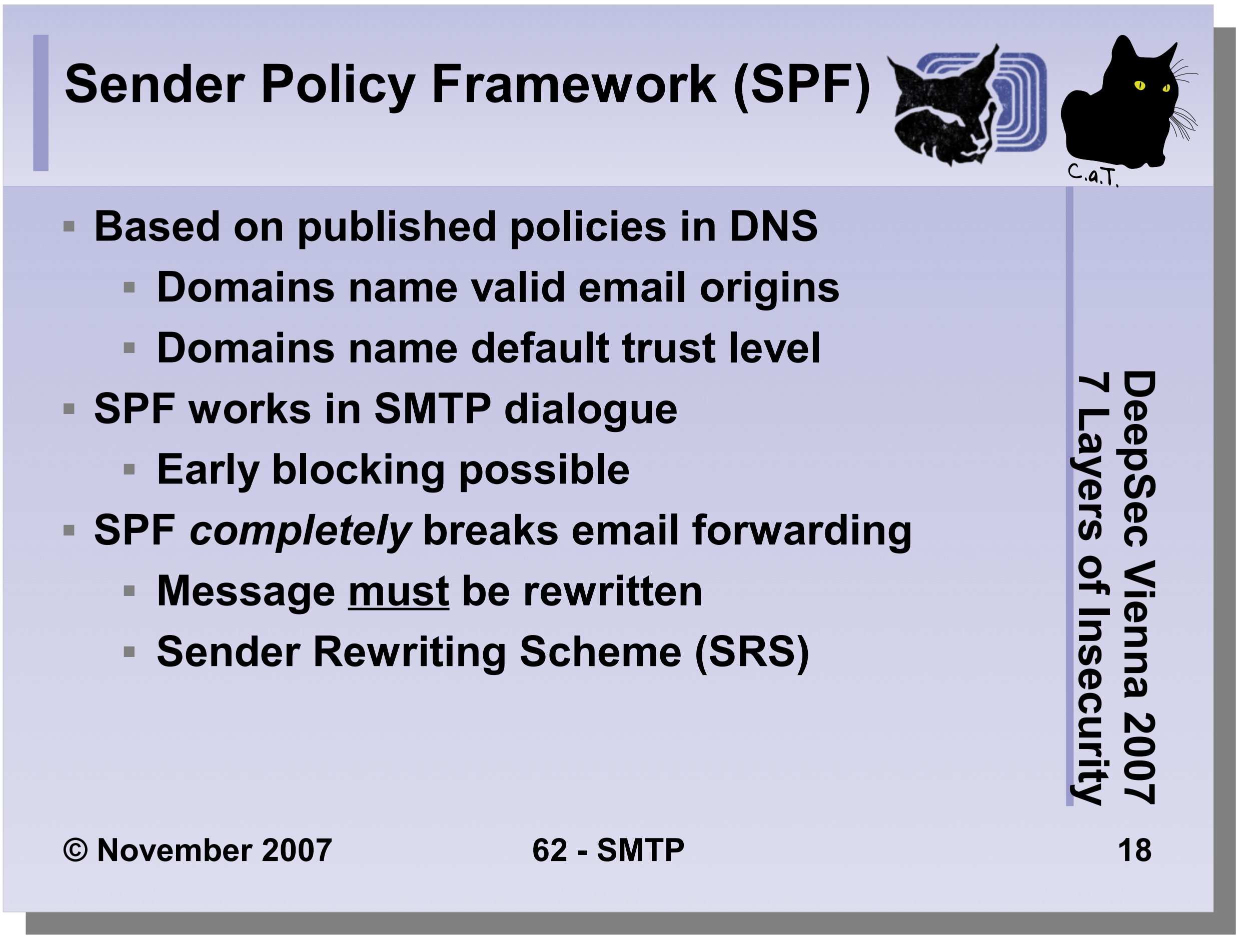


Domain Keys & DNS

- DomainKey-Signature header has fields: …d=example.net; s=dkim.key;…
- PK lookup: dkim.key._domainkey.example.net
- DNS security determines DKIM security
  - DNS attacks apply as well
  - Attacker may try to offer own key

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 62 - SMTP 17

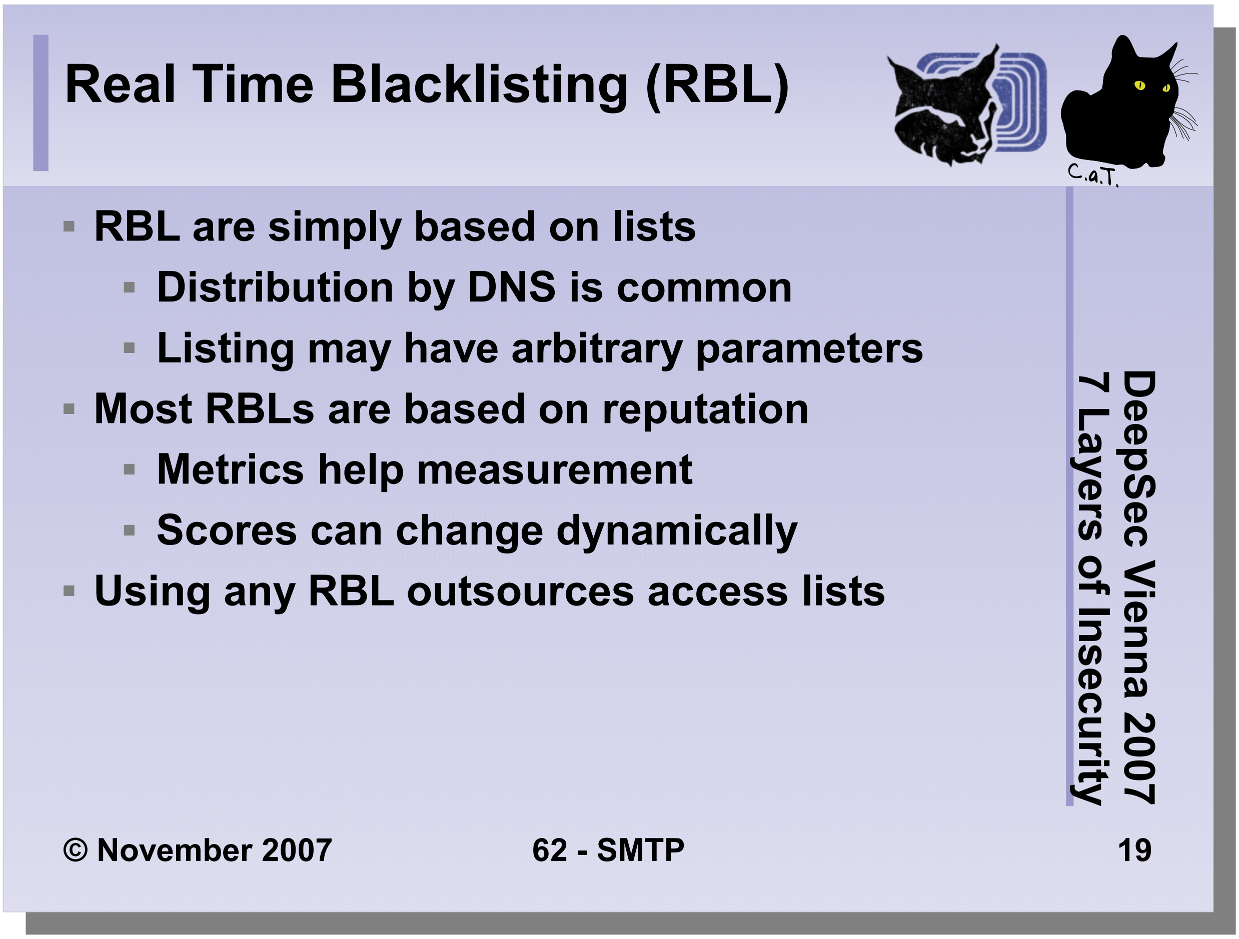


Sender Policy Framework (SPF)

- Based on published policies in DNS
  - Domains name valid email origins
  - Domains name default trust level
- SPF works in SMTP dialogue
  - Early blocking possible
- SPF *completely* breaks email forwarding
  - Message must be rewritten
  - Sender Rewriting Scheme (SRS)

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 62 - SMTP 18

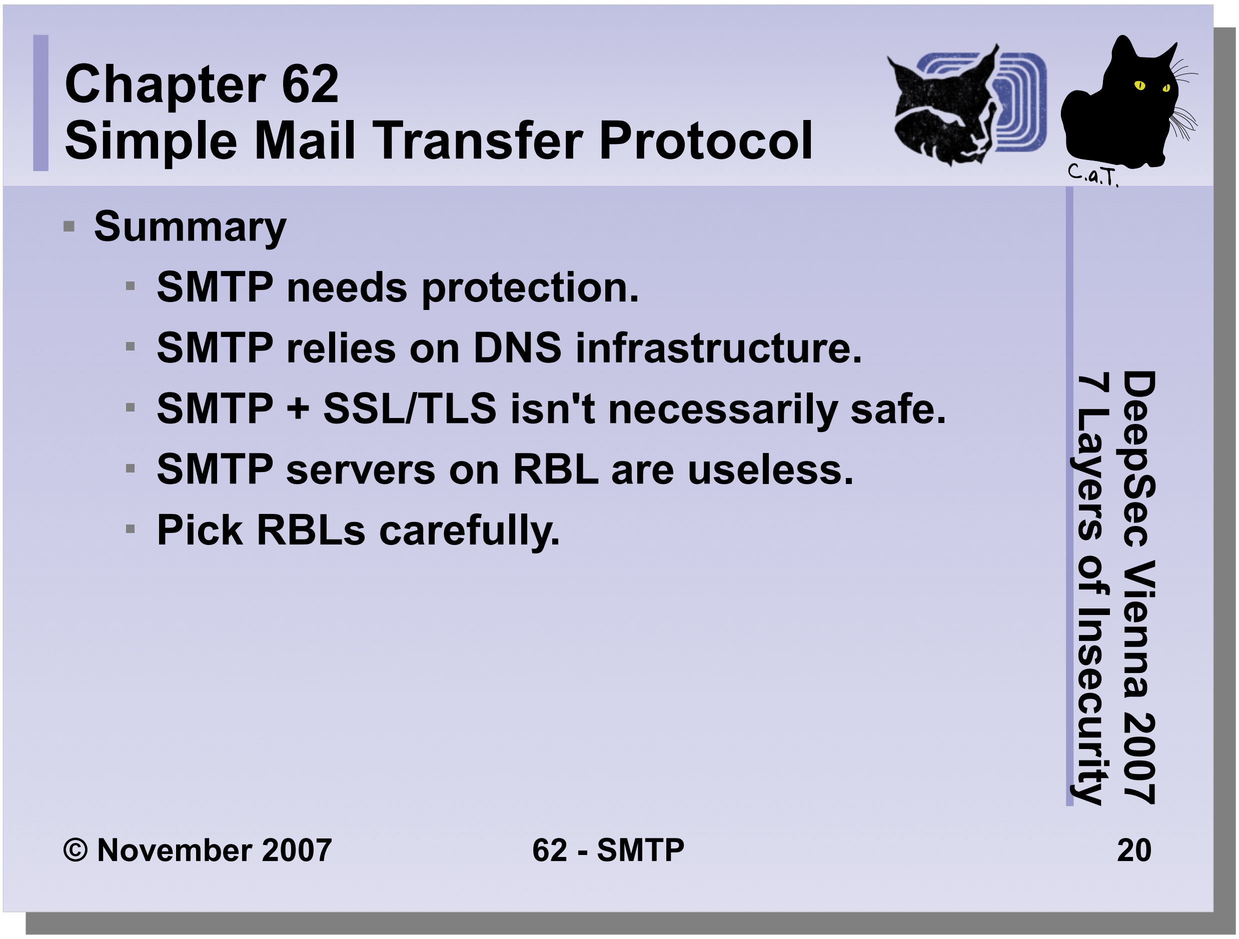


Real Time Blacklisting (RBL)

- RBL are simply based on lists
  - Distribution by DNS is common
  - Listing may have arbitrary parameters
- Most RBLs are based on reputation
  - Metrics help measurement
  - Scores can change dynamically
- Using any RBL outsources access lists

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 62 - SMTP 19



Chapter 62
Simple Mail Transfer Protocol

- Summary
  - SMTP needs protection.
  - SMTP relies on DNS infrastructure.
  - SMTP + SSL/TLS isn't necessarily safe.
  - SMTP servers on RBL are useless.
  - Pick RBLs carefully.

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 62 - SMTP 20

Thank You

- Questions?

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 62 - SMTP 21