Security Bugs in Protocols are Really Bad!

Marsh Ray

PhoneFactor

PhoneFactor

Protocol Bugs

Objectives

- Discuss the complexities in mitigating security bugs occurring in network protocols.
- Describe some current issues.
- Leave time for Q&A.

Protocol Bugs

Outline:

- Case Study: NTLM Credentials Forwarding
- Case Study: TLS Authentication Gap
- Conclusions

Case Study:

NTLM Credentials Forwarding

NTLM Credentials Forwarding

Problem:

Protocols using the NTLM and MS-CHAP (both v1 and v2) authentication schemes are subject to trivial credentials forwarding attacks.

- This is a separate issue from the various password-recovery attacks.

NTLM Credentials Forwarding

- This scheme is a natural expression of how Windows stores (non-Kerberos) credentials.

  It's used by a lot of stuff ...

NTLM Credentials Forwarding

- VPNs

L2TP

PPTP-MPPE

NTLM Credentials Forwarding

- email

POP3

SMTP

IMAP

NTLM Credentials Forwarding

- Remote desktop and telephony

RDP

SIP

NTLM Credentials Forwarding

- Web

HTTP

HTTPS

NTLM Credentials Forwarding

- Directory and single sign-on

LDAP

RADIUS

NTLM Credentials Forwarding

- Windows file sharing and RPC

SMB

CIFS

MS-RPC

MS-RPC/HTTP

NTLM Credentials Forwarding

- Other

MS SQL

MS Media Player

and last but not least...

NTLM Credentials Forwarding

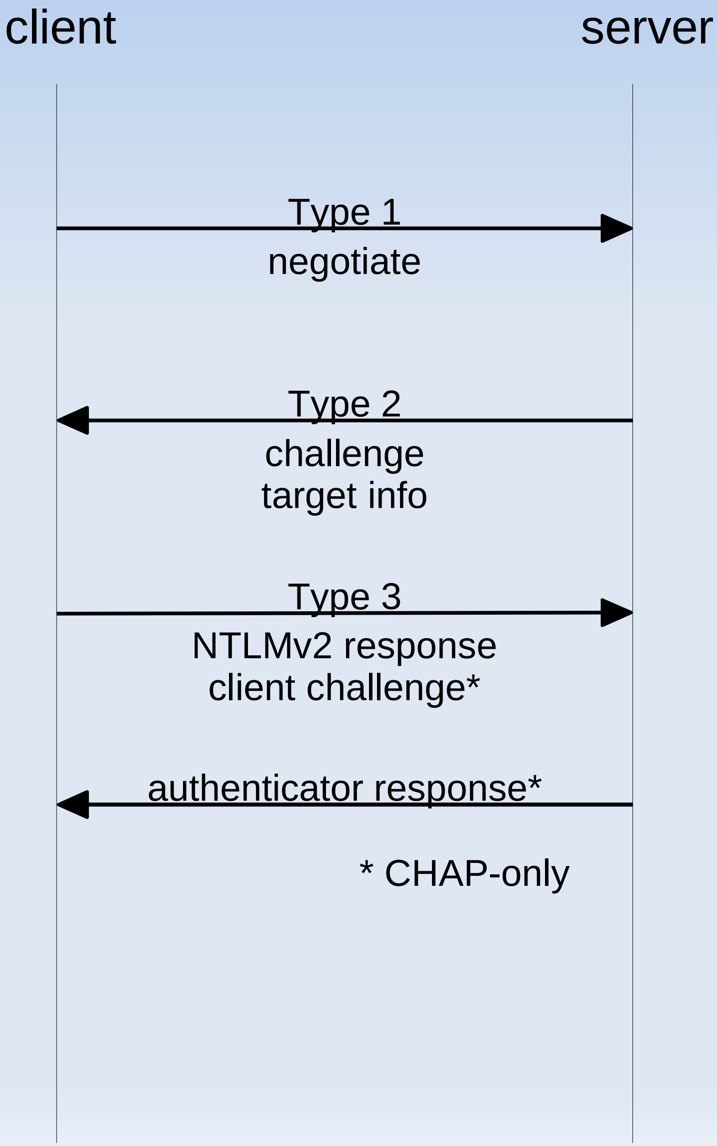
- Classics

FTP

Telnet

NTLM Credentials Forwarding

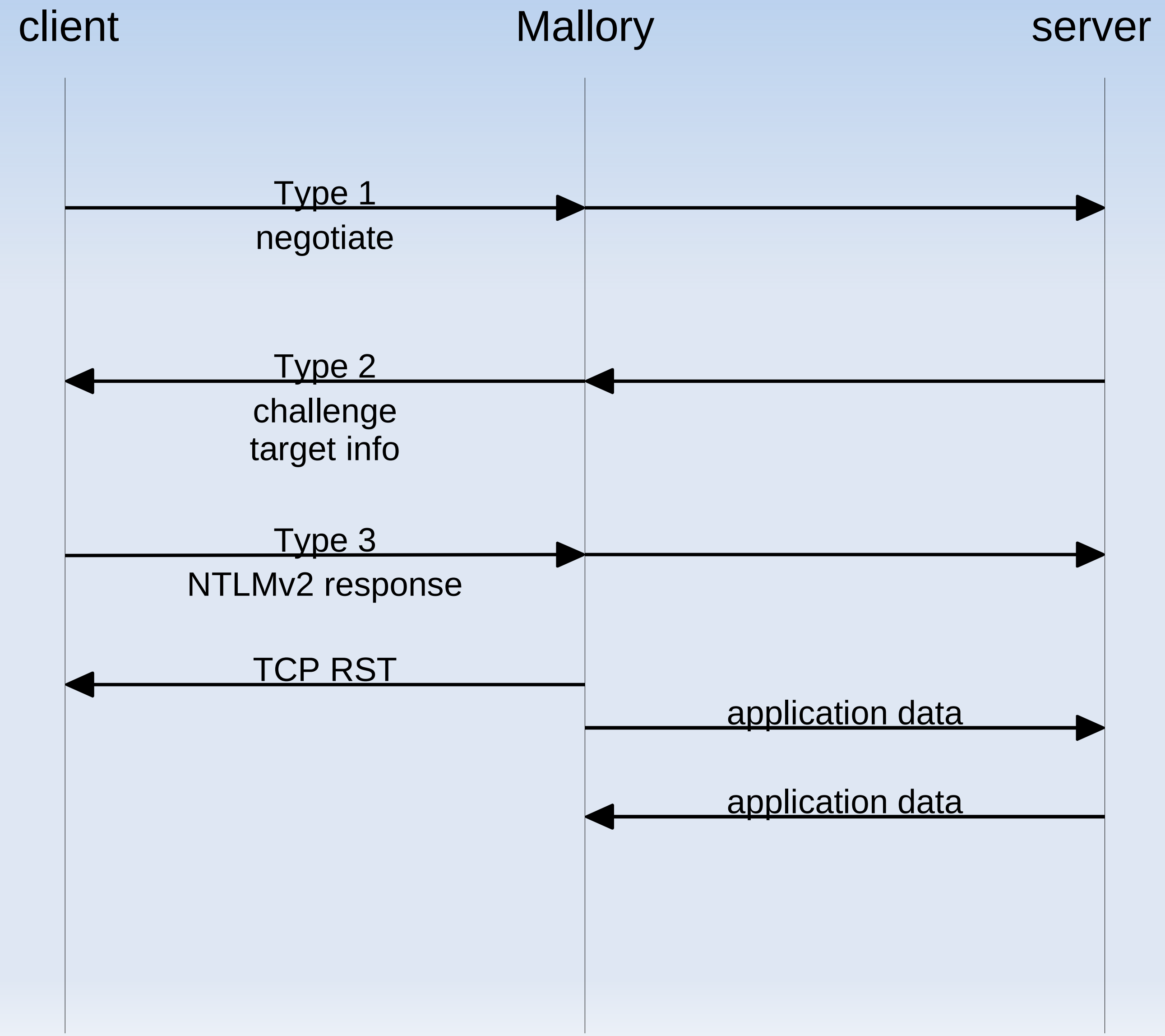
Normal Usage



PhoneFactor

NTLM Credentials Forwarding

The Attack!



NTLM Credentials Forwarding

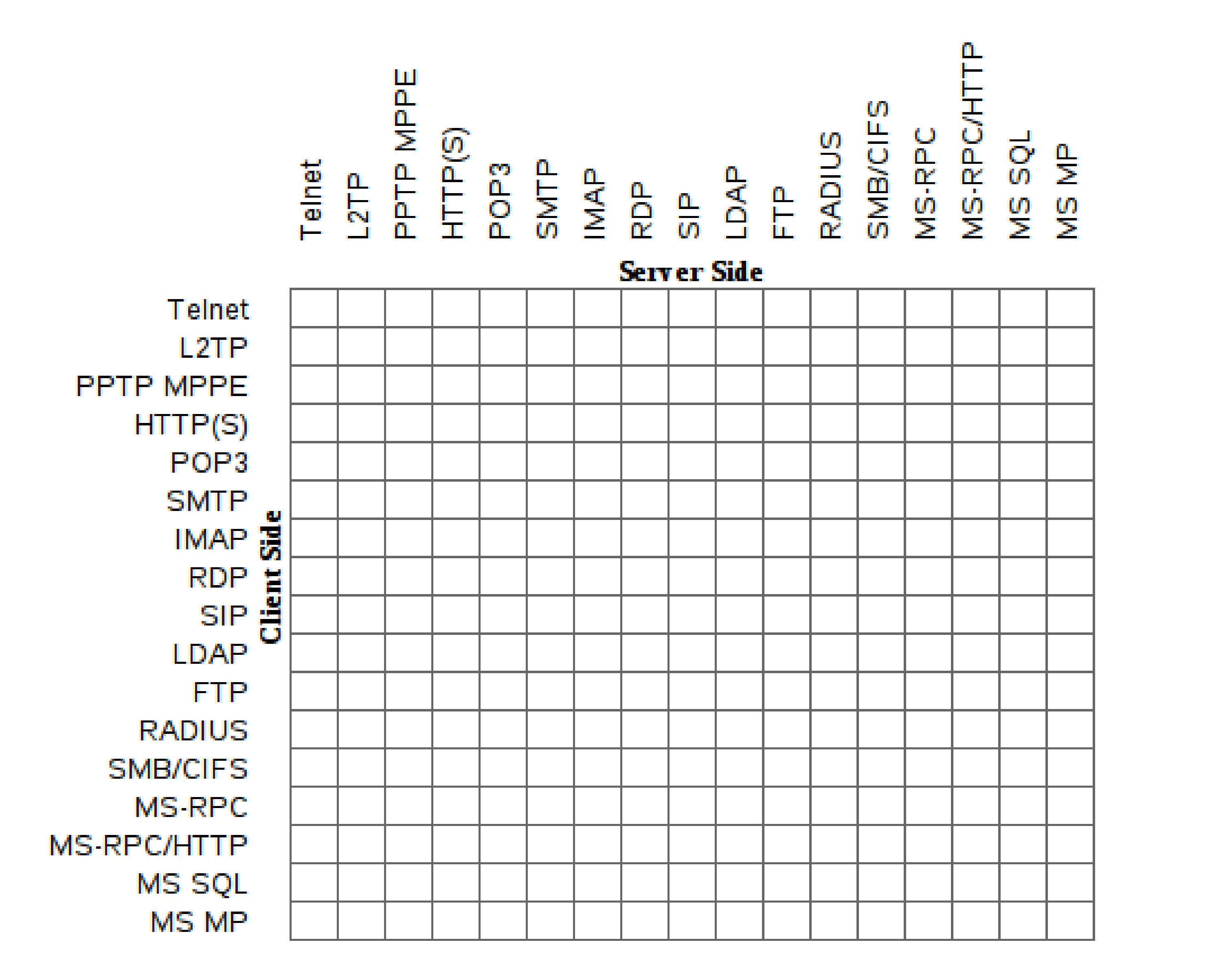
- How bad is it?
  - Alice connects to insecure WiFi with Windows
  - Mallory gets into corporate VPN

IT'S THAT BAD*

* Plausibly

NTLM Credentials Forwarding

- It's a cross-protocol attack:



Server Side

Client Side

	Telnet	L2TP	PPTP MPPE	HTTP(S)	POP3	SMTP	IMAP	RDP	SIP	LDAP	FTP	RADIUS	SMB/CIFS	MS-RPC	MS-RPC/HTTP	MS SQL	MS MP
Telnet																	
L2TP																	
PPTP MPPE																	
HTTP(S)																	
POP3																	
SMTP																	
IMAP																	
RDP																	
SIP																	
LDAP																	
FTP																	
RADIUS																	
SMB/CIFS																	
MS-RPC																	
MS-RPC/HTTP																	
MS SQL																	
MS MP																	

NTLM Credentials Forwarding

- So who knew?

> *It's been a mainstay of penteseters for a long time...*
>
> *...it always surpises people who take my Tactical Exploitation class and do the NTLM relay labs.*
>
> \- HD Moore

NTLM Credentials Forwarding

- So who knew?

  Microsoft, other vendors, and hackers have known about it *forever*.

NTLM Credentials Forwarding

1996

- Dominique Brezinski

  "A Weakness in CIFS Authentication"

NTLM Credentials Forwarding

1997

- Dominique Brezinski

  BlackHat

  "Security posture assessment of Windows NT networks"

NTLM Credentials Forwarding

1999

- Schneier, Mudge, Wagner

  Cryptanalysis of Microsoft's PPTP Authentication Extensions (MSCHAPv2)

  But discussion of credentials forwarding or MitM is conspicuously absent

- CVE-1999-1087 MS98-016

  IE interprets a 32-bit number as an Intranet zone IP address

NTLM Credentials Forwarding

2000

- DilDog - @stake

  Telnet NTLM Replay

- CVE-2000-0834 MS00-067

  Patch for "Windows 2000 Telnet Client NTLM Authentication" Vulnerability

NTLM Credentials Forwarding

2001

- Sir Dystic - Cult of the Dead Cow

  @lantacon

  SMBRelay

- CVE-2001-0003 MS01-001

  Patch for MS Office "Web Extender Client" to follow IE settings for NTLM

NTLM Credentials Forwarding

2004

- Jesse Burns - iSEC

  NTLM Authentication Unsafe

  HTTP to SMB attack demo

NTLM Credentials Forwarding

2007

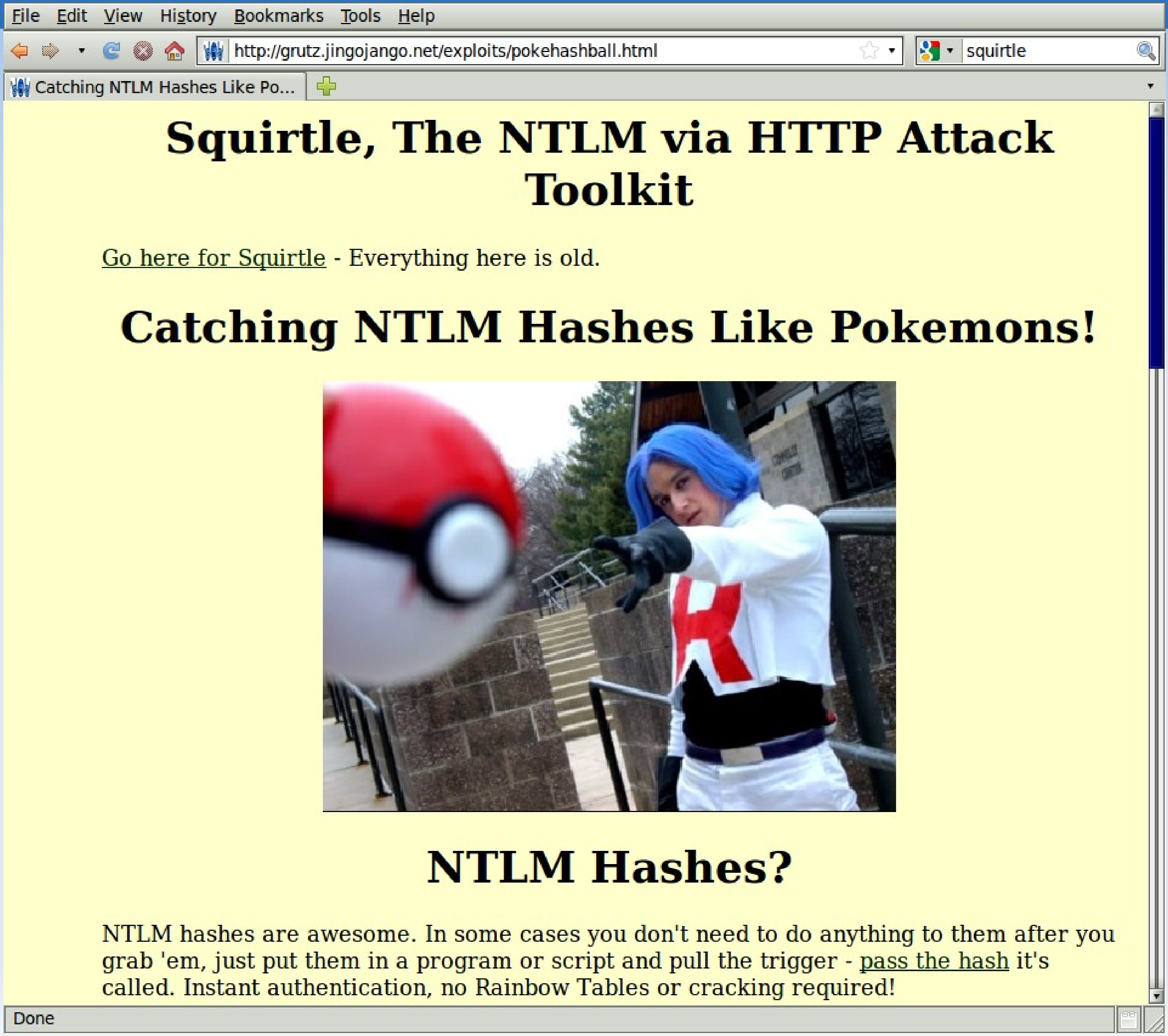
- Grutzmacher

  Squirtle

NTLM Credentials Forwarding

- Squirtle
  - Water-type Pokémon
  - Ability: Torrent
    - If < 33% HP remaining, power increased by 1.5x
  - Domesticated
    - well-behaved
    - loyal
  - Evolves into Wartortle

NTLM Credentials Forwarding


File Edit View History Bookmarks Tools Help
http://grutz.jingojango.net/exploits/pokehashball.html
squirtle
Catching NTLM Hashes Like Po...
Done

Squirtle, The NTLM via HTTP Attack Toolkit

Go here for Squirtle - Everything here is old.

Catching NTLM Hashes Like Pokemons!

NTLM Hashes?

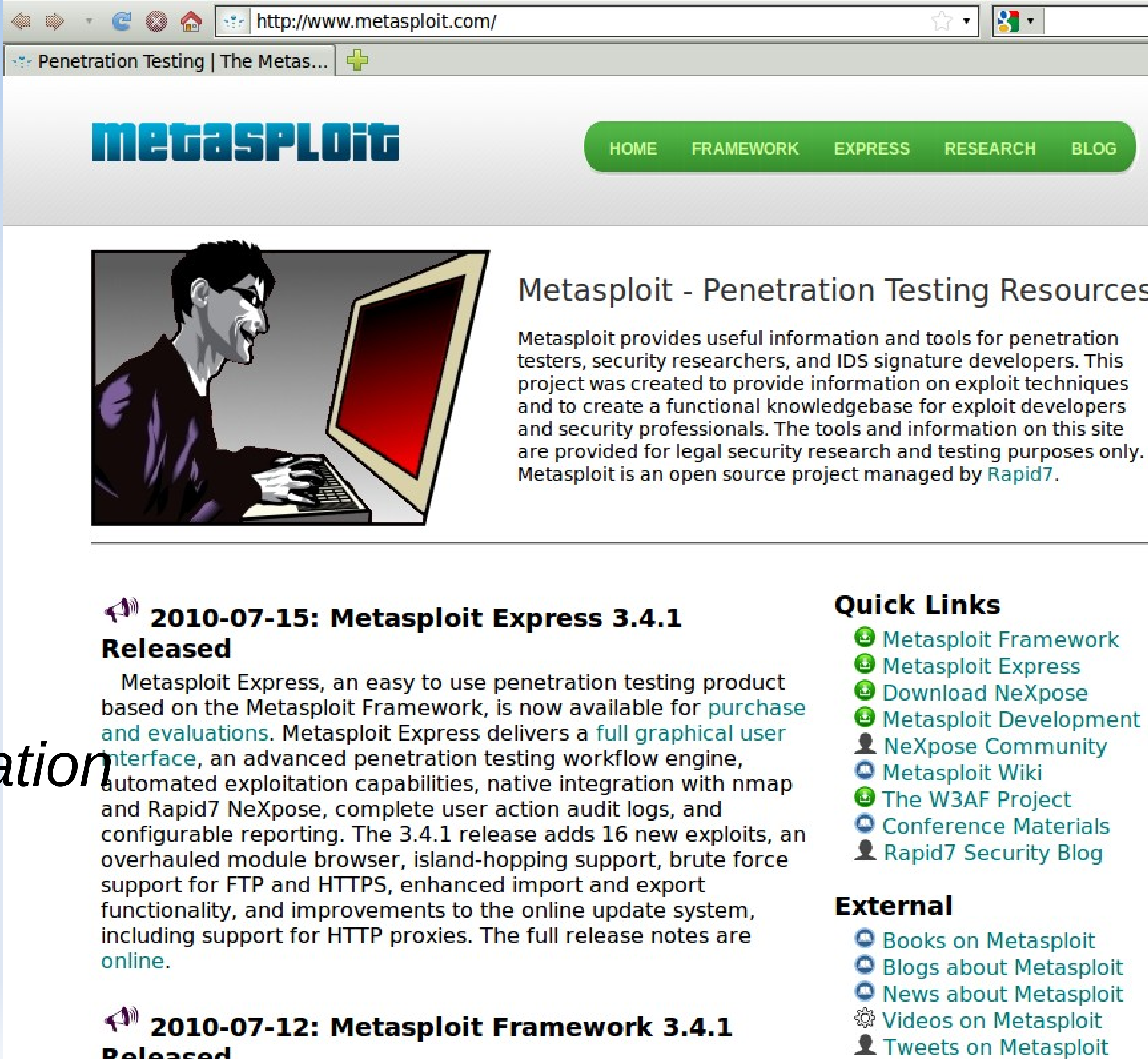
NTLM hashes are awesome. In some cases you don't need to do anything to them after you grab 'em, just put them in a program or script and pull the trigger - pass the hash it's called. Instant authentication, no Rainbow Tables or cracking required!

NTLM Credentials Forwarding

2007

- HTTP to SMB added to Metasploit

- HD Moore, valsmith BlackHat *Tactical Exploitation*



http://www.metasploit.com/
Penetration Testing | The Metas...
metasploit
HOME
FRAMEWORK
EXPRESS
RESEARCH
BLOG

Metasploit - Penetration Testing Resources

Metasploit provides useful information and tools for penetration testers, security researchers, and IDS signature developers. This project was created to provide information on exploit techniques and to create a functional knowledgebase for exploit developers and security professionals. The tools and information on this site are provided for legal security research and testing purposes only. Metasploit is an open source project managed by Rapid7.

2010-07-15: Metasploit Express 3.4.1 Released

Metasploit Express, an easy to use penetration testing product based on the Metasploit Framework, is now available for purchase and evaluations. Metasploit Express delivers a full graphical user interface, an advanced penetration testing workflow engine, automated exploitation capabilities, native integration with nmap and Rapid7 NeXpose, complete user action audit logs, and configurable reporting. The 3.4.1 release adds 16 new exploits, an overhauled module browser, island-hopping support, brute force support for FTP and HTTPS, enhanced import and export functionality, and improvements to the online update system, including support for HTTP proxies. The full release notes are online.

2010-07-12: Metasploit Framework 3.4.1 Released

Quick Links

- Metasploit Framework
- Metasploit Express
- Download NeXpose
- Metasploit Development
- NeXpose Community
- Metasploit Wiki
- The W3AF Project
- Conference Materials
- Rapid7 Security Blog

External

- Books on Metasploit
- Blogs about Metasploit
- News about Metasploit
- Videos on Metasploit
- Tweets on Metasploit

NTLM Credentials Forwarding

2008

- Eric Rachner

  Exploits HTTP-HTTP

NTLM Credentials Forwarding

2008

- CVE-2008-3009 MS08-076

  Windows Media do not use the SPN for validating replies

- CVE-2008-3010 MS08-076

  Windows Media associates ISATAP addresses with Intranet zone

- CVE-2008-4037 MS08-068

  SMB credential reflection protection

NTLM Credentials Forwarding

2009

- CVE-2009-0550 MS09-013

  WinHTTP doesn't correctly opt-in to the NTLM reflection protection

- CVE-2009-0550 MS09-014

  WinINet doesn't correctly opt-in to the NTLM reflection protection

- CVE-2009-1930 MS09-042

  Telnet protocol doesn't correctly opt-in to the NTLM reflection protection

NTLM Credentials Forwarding

2010

- Hernan Ocha, Augustin Azubel

  BlackHat

  Windows' SMB PRNG is defective

  - CVE-2010-0231

NTLM Credentials Forwarding

- CVE-2005-0147

  Firefox responds to proxy auth requests from arbitrary servers

- CVE-2009-3983

  Firefox allows remote attackers to replay NTLM credentials of the user

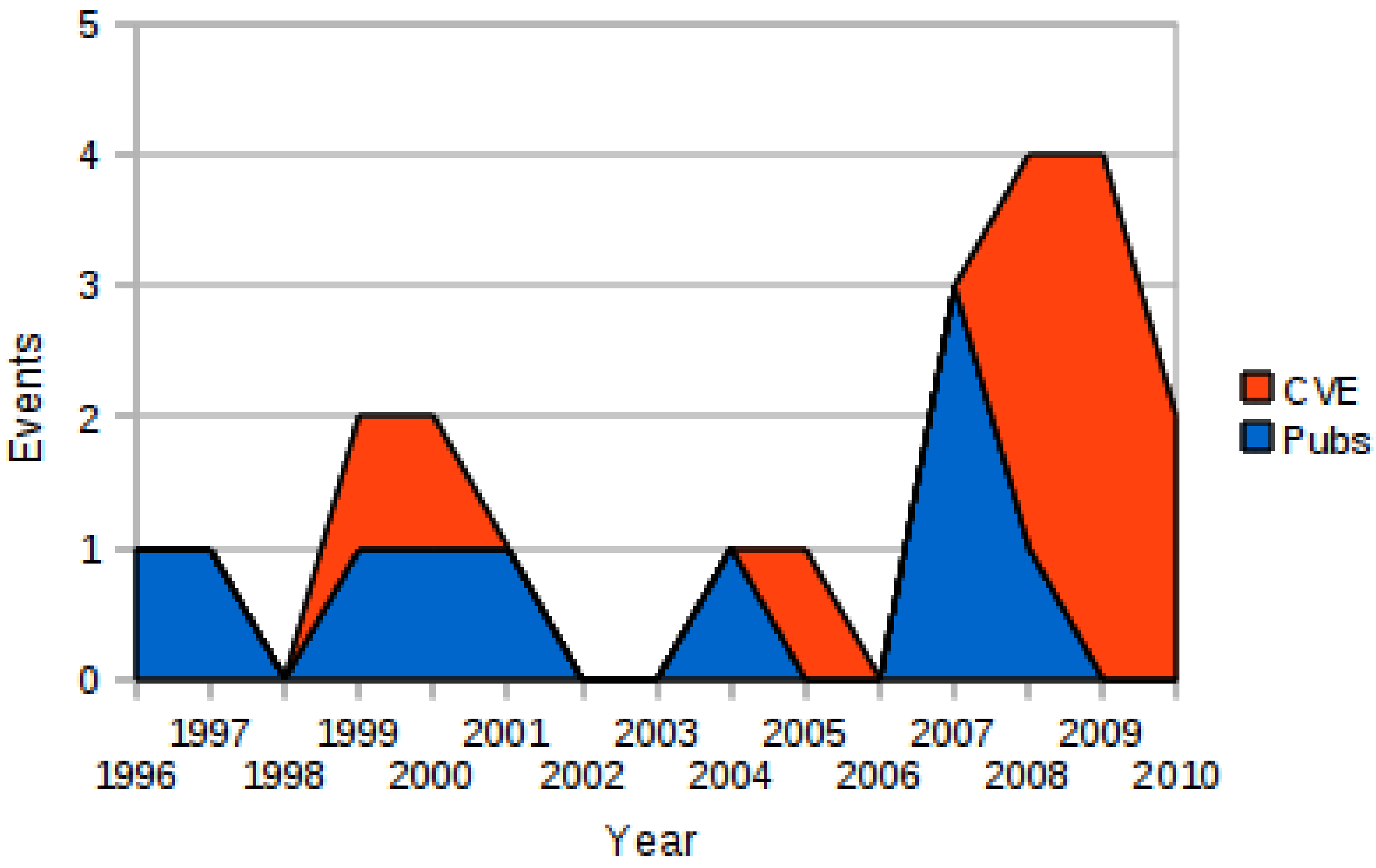
- CVE-2010-1413

  Webkit sends NTLM in unspecified circumstances.

NTLM Credentials Forwarding

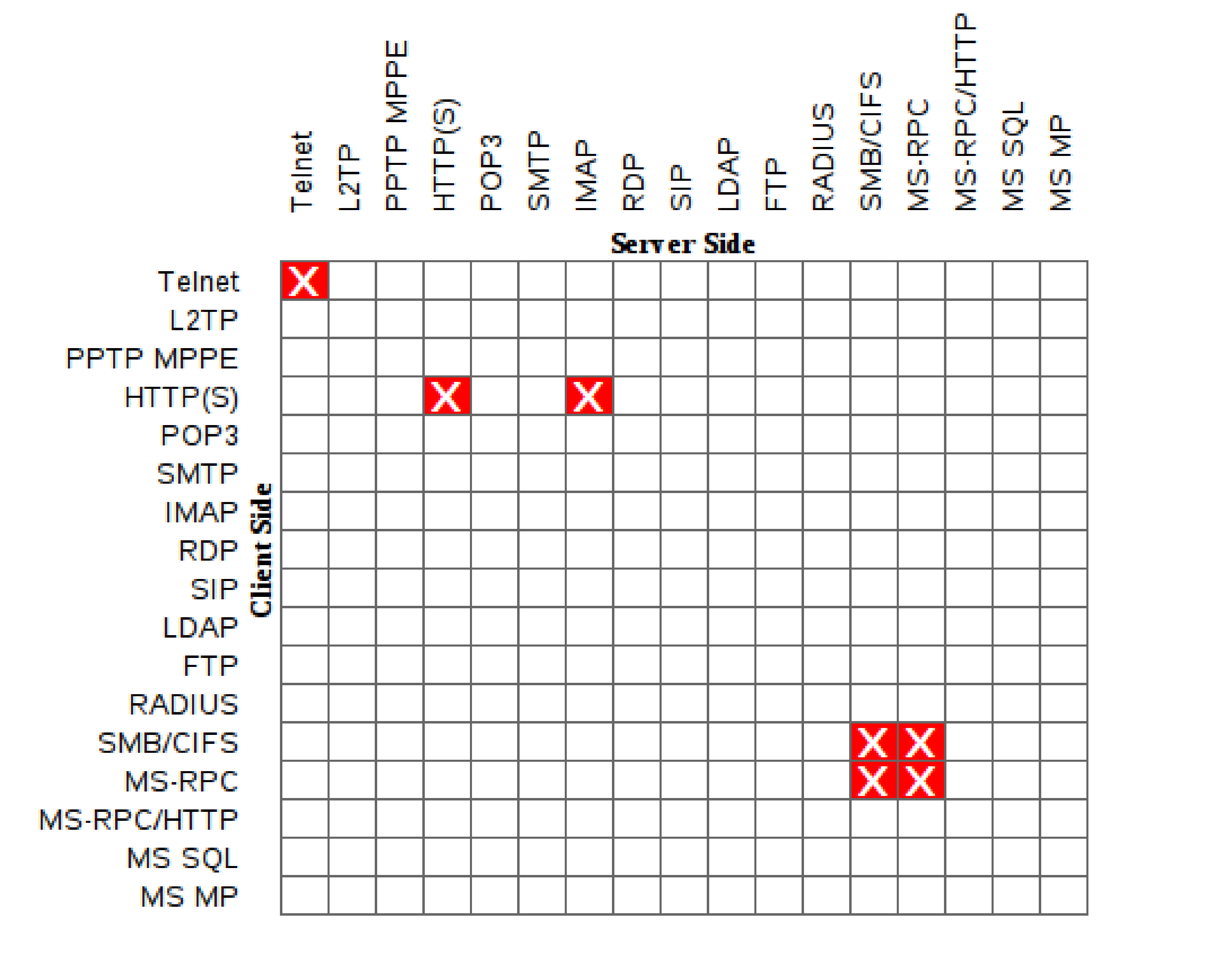
- Presentations, Publications, and CVEs

Year	Pubs	CVE	total
1996	1		1
1997	1		1
1998			
1999	1	1	2
2000	1	1	2
2001	1		1
2002			
2003			
2004	1		1
2005		1	1
2006			
2007	3		3
2008	1	3	4
2009		4	4
2010		2	2



NTLM Credentials Forwarding

- Most attack space remains to be explored:



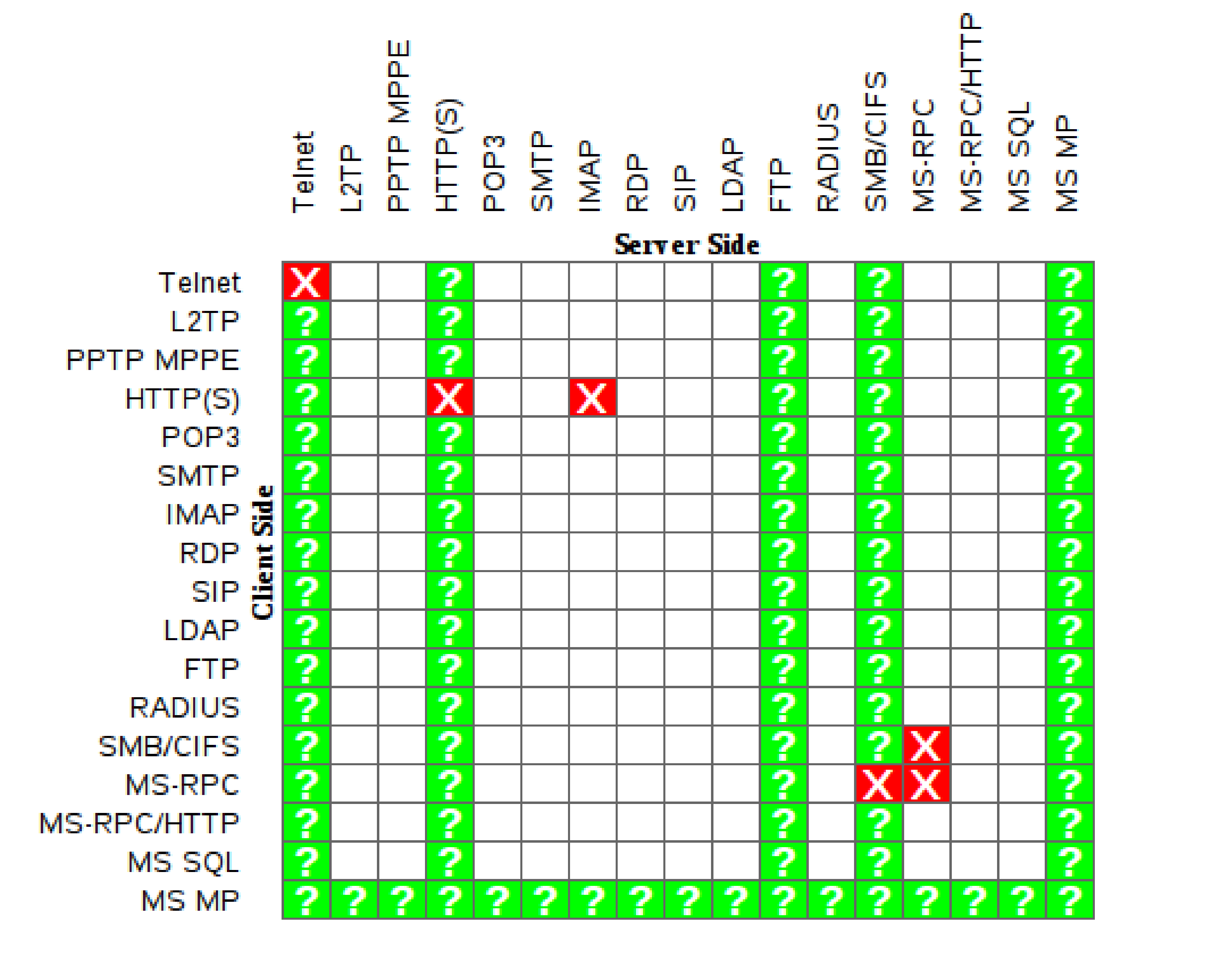
Server Side

Client Side

	Telnet	L2TP	PPTP MPPE	HTTP(S)	POP3	SMTP	IMAP	RDP	SIP	LDAP	FTP	RADIUS	SMB/CIFS	MS-RPC	MS-RPC/HTTP	MS SQL	MS MP
Telnet	X																
L2TP																	
PPTP MPPE																	
HTTP(S)				X			X										
POP3																	
SMTP																	
IMAP																	
RDP																	
SIP																	
LDAP																	
FTP																	
RADIUS																	
SMB/CIFS													X	X			
MS-RPC													X	X			
MS-RPC/HTTP																	
MS SQL																	
MS MP																	

NTLM Credentials Forwarding

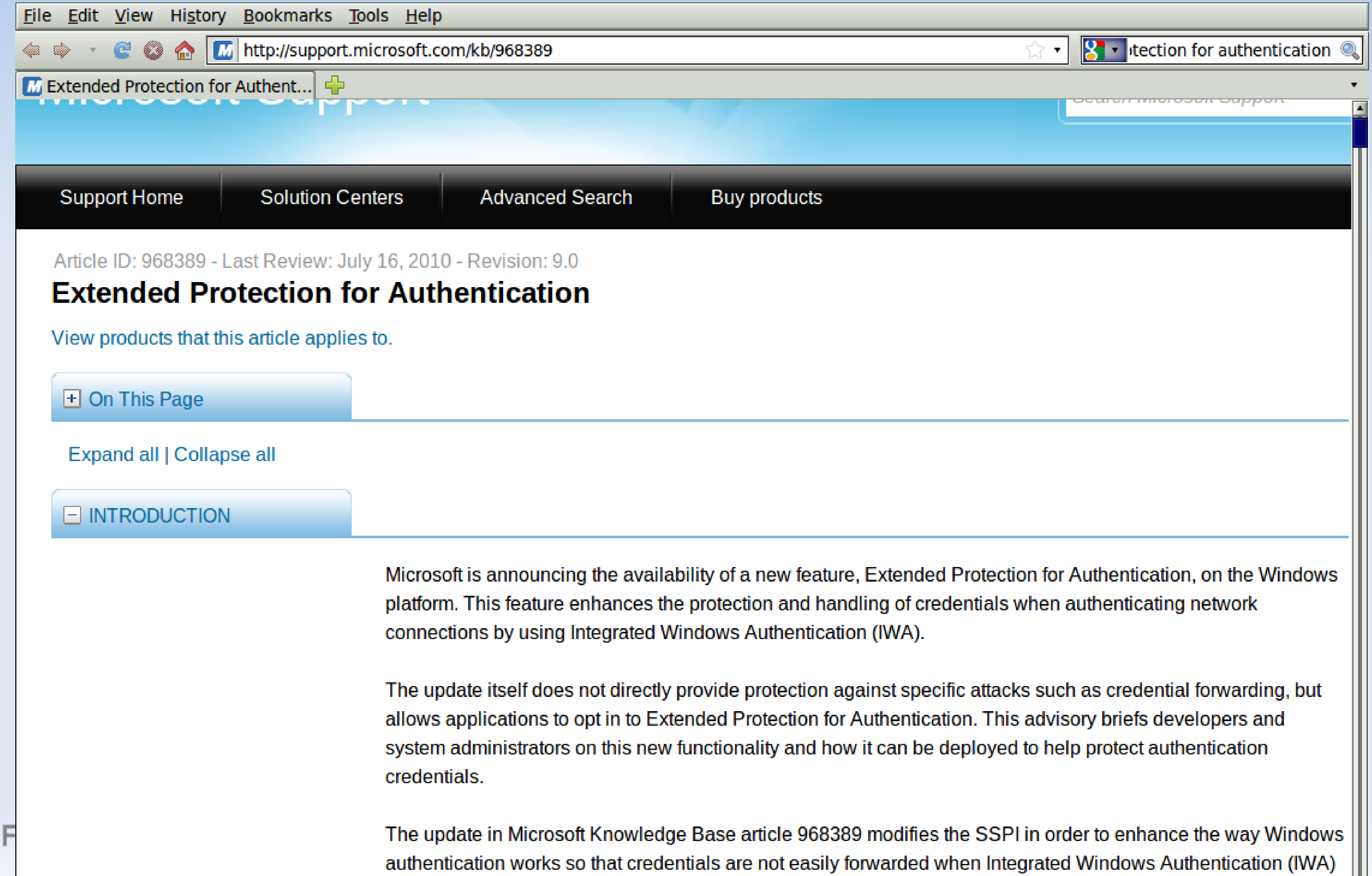
- Some mitigations have been released:



Client Side	Server Side																
	Telnet	L2TP	PPTP MPPE	HTTP(S)	POP3	SMTP	IMAP	RDP	SIP	LDAP	FTP	RADIUS	SMB/CIFS	MS-RPC	MS-RPC/HTTP	MS SQL	MS MP
Telnet	X			?							?		?				?
L2TP	?			?							?		?				?
PPTP MPPE	?			?							?		?				?
HTTP(S)	?			X			X				?		?				?
POP3	?			?							?		?				?
SMTP	?			?							?		?				?
IMAP	?			?							?		?				?
RDP	?			?							?		?				?
SIP	?			?							?		?				?
LDAP	?			?							?		?				?
FTP	?			?							?		?				?
RADIUS	?			?							?		?				?
SMB/CIFS	?			?							?		?	X			?
MS-RPC	?			?							?		X	X			?
MS-RPC/HTTP	?			?							?		?				?
MS SQL	?			?							?		?				?
MS MP	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?

NTLM Credentials Forwarding

- MS Extended Protection for Authentication


File Edit View History Bookmarks Tools Help
http://support.microsoft.com/kb/968389
ıtection for authentication
Extended Protection for Authent...
Support Home
Solution Centers
Advanced Search
Buy products

Article ID: 968389 - Last Review: July 16, 2010 - Revision: 9.0

Extended Protection for Authentication

View products that this article applies to.

⊞ On This Page

Expand all | Collapse all

⊟ INTRODUCTION

Microsoft is announcing the availability of a new feature, Extended Protection for Authentication, on the Windows platform. This feature enhances the protection and handling of credentials when authenticating network connections by using Integrated Windows Authentication (IWA).

The update itself does not directly provide protection against specific attacks such as credential forwarding, but allows applications to opt in to Extended Protection for Authentication. This advisory briefs developers and system administrators on this new functionality and how it can be deployed to help protect authentication credentials.

The update in Microsoft Knowledge Base article 968389 modifies the SSPI in order to enhance the way Windows authentication works so that credentials are not easily forwarded when Integrated Windows Authentication (IWA)

NTLM Credentials Forwarding

- MS Extended Protection for Authentication
  - [These updates] allow web clients using the Windows HTTP Services, IIS web servers and applications based on http.sys to use this feature.
  - Deployment of EAP must happen on both the client and server for any given application. If only one side supports the feature, the connection will not benefit from the additional protection offered.

- blogs.technet.com

NTLM Credentials Forwarding

- Mitigations
  - No fix can be completely effective without breaking backwards compatibility
  - Patching one protocol at a time to retrofit opt-in security is not a winning strategy
  - If back-compat must be broken, do it once and end up with a comprehensive fix!
    - E.g., NTLMv1 -> NTLMv2 !

NTLM Credentials Forwarding

Conclusion

- The best choice would have been to begin transitioning to NTLMv3 back in 1997.

Case Study:
TLS Authentication Gap

Conclusions

Protocol Bugs

Common features

- Take a long time to be identified

  often only after a large installed base exists

Protocol Bugs

Common features

- Difficult to assess
  - Minor weaknesses at different layers combine to form serious vulnerabilities
  - Initially unclear how to assess severity
  - Not always a simple test to determine a system's susceptibility
  - Attention-getting attacks (e.g. password cracking) may distract from the core vulnerability

Protocol Bugs

Common features

- Seem to be subtle
  - Overlooked by multiple reviewers
  - Research not always accepted immediately
  - Successful exploit may seem to require "Mission Impossible"-type planning

    But this silently changes over time!

Protocol Bugs

Common features

Difficult to mitigate

- The need to maintain backwards compatibility usually prevents an effective fix.

  People wouldn't apply such a patch

  A complete fix can mean patching every client and every server in the world.

  Sometimes requires a complex multistage roll-out:

  Phase 1 - a year or more

  Phase 2 - a decade

Protocol Bugs

Common features

- Built into embedded devices

  Firmware, even hardware

- Difficult to detect
  - Flaw may be hidden by encryption
  - A successful exploit may be indistinguishable from a valid transaction or simple packet loss.

Protocol Bugs

- Contact:

  marsh@extendedsubset.com

  marsh@phonefactor.com

  @marshray Twitter

  marsh on silc.hick.org