

20 Years of Network and Distributed Systems Security: the Good, the Bad, and the Ugly

Richard A. Kemmerer

Computer Security Group

Department of Computer Science

University of California, Santa Barbara

<http://seclab.cs.ucsb.edu>



NDSS13

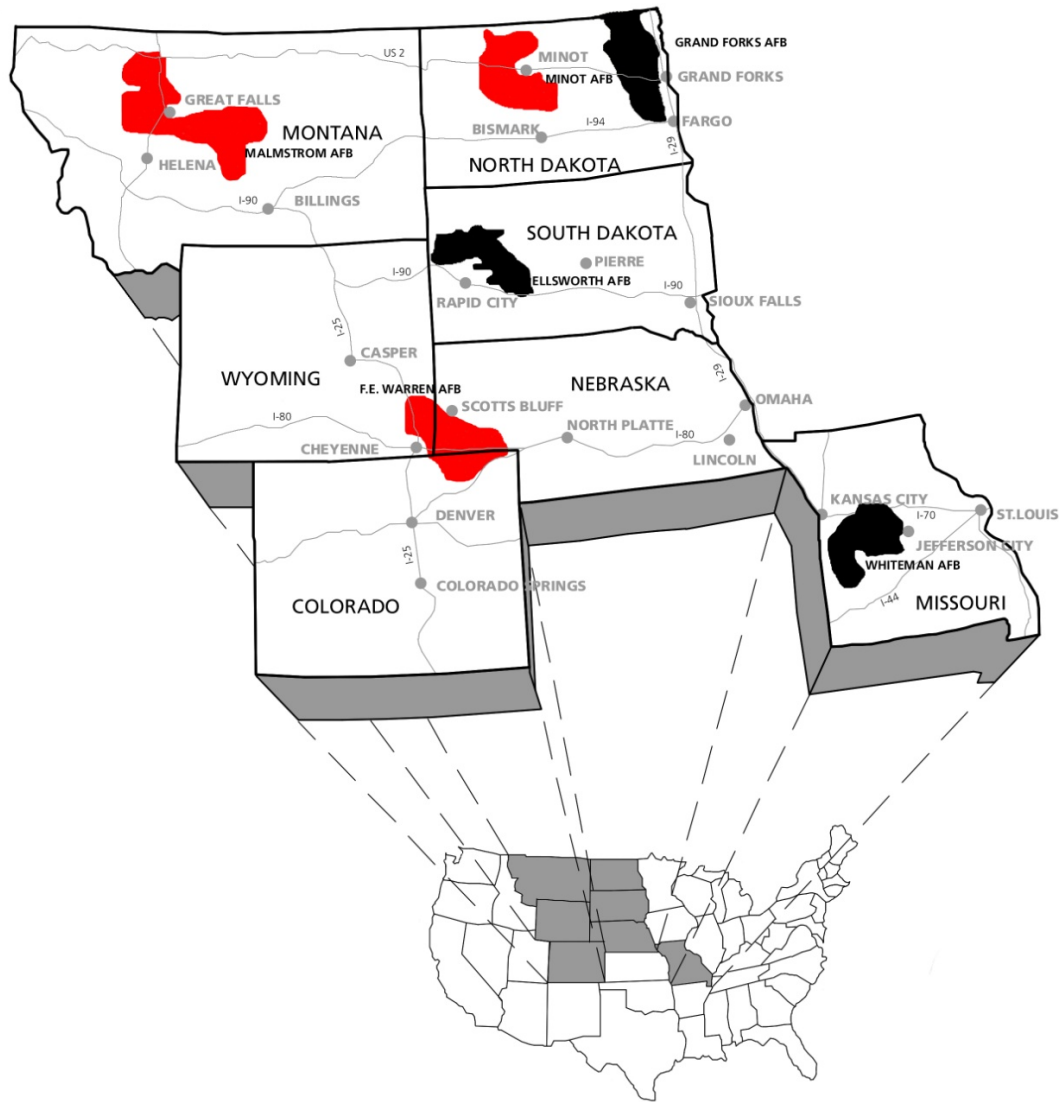


February, 25,2013

Why me?

- My first NDSS was 2006
- First distributed system work 1967

Distributed in the Midwest



Secure Transport Service

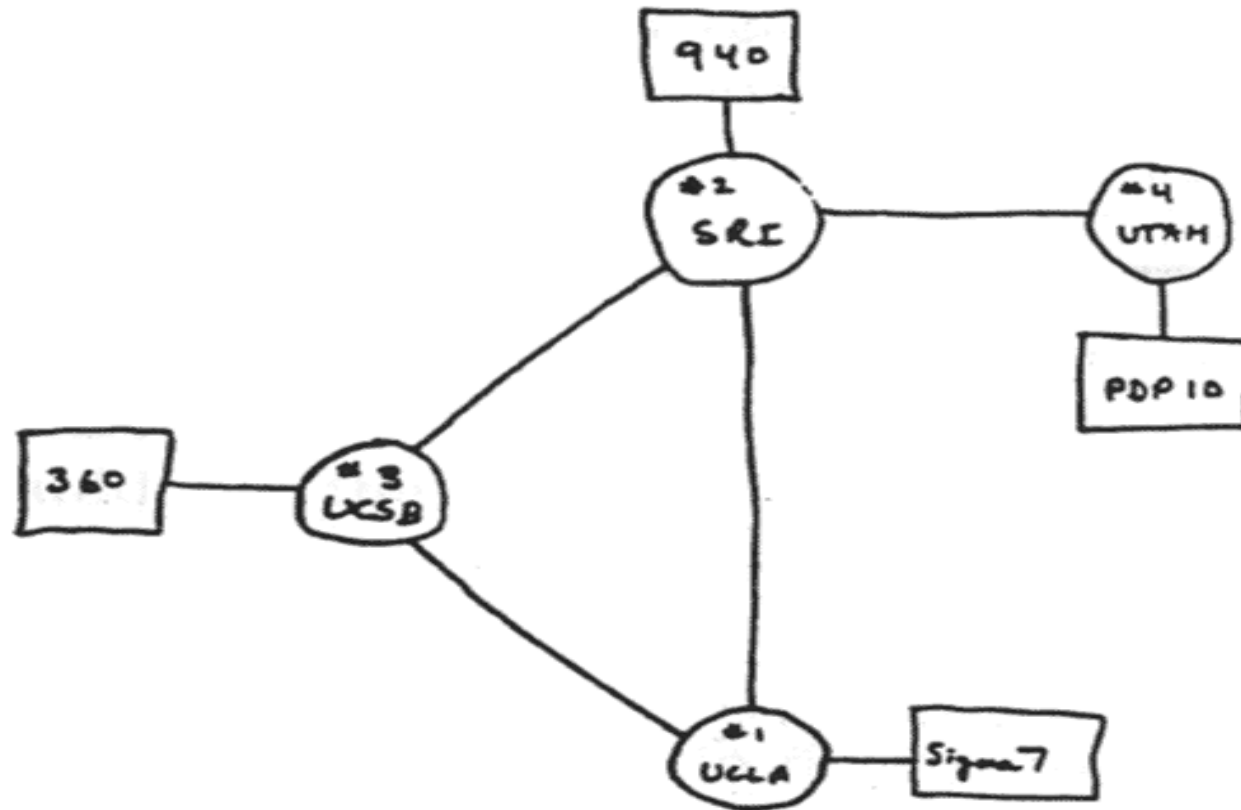


Minute III ICBM





1970 Moved to UCLA



THE ARPANET NETWORK

DEC 1969

Simulations for Arpanet Protocols

- Packet switching
- Packet switching with cut-through
- Aloha (pure and slotted)
- Carrier sense multiple access (CSMA)
- Packet radio

Hazeltine portable packet radio

- This mobile field radio for the military used ARPA's pioneering packet radio network. Each unit created a new node that extended the network.





SRI truck for portable packet radio experiments



Victim of DEC Spam of 1978

- Sent by aggressive DEC marketer to every Arpanet address on the west coast
- Sent from SNDMSG
- Limited space for To, CC, and Subject fields
- Manually entered addresses starting in the Subject, which overflowed into the To header, which overflowed into the CC header, which overflowed into the Body, because would only accept 320 addresses

Header

Mail-from: DEC-MARLBORO rcvd at 3-May-78 0955-PDT

Date: 1 May 1978 1233-EDT

From: THUERK at DEC-MARLBORO

Subject: ADRIAN@SRI-KL

To: DDAY at SRI-KL, DAY at SRI-KL, DEBOER at UCLA-CCN,

To: WASHDC at SRI-KL, LOGICON at USC-ISI, SDAC at USC-ISI,

To: DELDO at USC-ISI, DELEOT at USC-ISI, DELFINO at USC-ISI,

To: DENICOFF at USC-ISI, DESPAIN at USC-ISI, DEUTSCH at SRI-KL,

To: DEUTSCH at PARC-MAXC, EMY at CCA-TENEX, DIETER at USC-ISIB,

To: DINES at AMES-67, MERADCON at SRI-KL, EPG-SPEC at SRI-KA,

To: DIVELY at SRI-KL, DODD at USC-ISI, DONCHIN at USC-ISIC,

To: JED at LLL-COMP, DORIN at CCA-TENEX, NYU at SRI-KA,

To: DOUGHERTY at USC-ISI, PACOMJ6 at USC-ISI,

To: DEBBY at UCLA-SECURITY, BELL at SRI-KL, JHANNON at SRI-KA,

To: DUBOIS at USC-ISI, DUDA at SRI-KL, POH at USC-ISI,

To: LES at SU-AI, EAST at BBN-TENEX, DEASTMAN at USC-ECL,

To: EBISU at I4-TENEX, NAC at USC-ISIE, ECONOMIDIS at I4-TENEX,

To: WALSH at SRI-KL, GEDWARDS at SRI-KL, WEDWARDS at USC-ISI,

To: NUSC at SRI-KL, RM at SU-AI, ELKIND at PARC-MAXC,

Me

To: KALTGRAD at UCLA-ATS, MARK at UCLA-SECURITY, RAK at SU-AI,
To: KASTNER at USC-ISIB, KATT at USC-ISIB,
To: UCLA-MNC at USC-ISI, ALAN at PARC-MAXC, KEENAN at USC-ISI,
To: KEHL at UCLA-CCN, KELLEY at SRI-KL, BANANA at I4-TENEX,
To: KELLOGG at USC-ISI, DDI at USC-ISI, KEMERY at SRI-KL,
To: KEMMERER at UCLA-ATS, PARVIZ at UCLA-ATS, KING at SUMEX-AIM,
To: KIRSTEIN at USC-ISI, SDC at UCLA-SECURITY,
To: KLEINROCK at USC-ISI, KLEMBA at SRI-KL, CSK at USC-ISI,
To: KNIGHT at SRI-KL, KNOX at USC-ISI, KODA at USC-ISIB,
To: KODANI at AMES-67, KOOIJ at USC-ISI, KREMERS at SRI-KL,
To: BELL at SRI-KL, KUNZELMAN at SRI-KL, PROJX at SRI-KL,
To: LAMPSON at PARC-MAXC, SDL at RAND-UNIX, JOJO at SRI-KL,
To: SDC at USC-ISI, NELC3030 at USC-ISI,
To: LEDERBERG at SUMEX-AIM, LEDUC at SRI-KL, JSLEE at USC-ECL,
To: JACOBS at USC-ISIE, WREN at USC-ISIB, LEMONS at USC-ISIB,
To: LEUNG at SRI-KL, J33PAC at USC-ISI, LEVIN at USC-ISIB,
To: LEVINTHAL at SUMEX-AIM, LICHTENBERGER at I4-TENEX,
To: LICHTENSTEIN at USC-ISI, LIDDLE at PARC-MAXC,
To: LIEB at USC-ISIB, LIEBERMAN at SRI-KL, STANL at USC-ISIE,

Overflow into CC and Body

To: MASON at USC-ISIB, MATHIS at SRI-KL, MAYNARD at USC-ISIC,
To: MCBREARTY at SRI-KL, MCCALL at SRI-KA, MCCARTHY at SU-AI,
To: MCCLELLAND at USC-ISI, DORIS at RAND-UNIX, MCCLURG at SRI-KL,
To: JOHN at I4-TENEX, MCCREIGHT at PARC-MAXC, MCCRUMB at USC-ISI,
To: DRXTE at SRI-KA
cc: BPM at SU-AI

MCKINLEY@USC-ISIB
MMCM@SRI-KL
OT-ITS@SRI-KA
BELL@SRI-KL
MEADE@SRI-KL
MARTIN@USC-ISI
MERRILL@BBN-TENEX
METCALFE@PARC-MAXC
JMETZGER@USC-ISIB
MICHAEL@USC-ISIC
CMILLER@SUMEX-AIM

ZOLOTOW@SRI-KL

ZOSEL@LLL-COMP

DIGITAL WILL BE GIVING A PRODUCT PRESENTATION OF THE NEWEST MEMBERS OF THE DECSYSTEM-20 FAMILY; THE DECSYSTEM-2020, 2020T, 2060, AND 2060T. THE DECSYSTEM-20 FAMILY OF COMPUTERS HAS EVOLVED FROM THE TENEX OPERATING SYSTEM AND THE DECSYSTEM-10 <PDP-10> COMPUTER ARCHITECTURE. BOTH THE DECSYSTEM-2060T AND 2020T OFFER FULL ARPANET SUPPORT UNDER THE TOPS-20 OPERATING SYSTEM. THE DECSYSTEM-2060 IS AN UPWARD EXTENSION OF THE CURRENT DECSYSTEM 2040 AND 2050 FAMILY. THE DECSYSTEM-2020 IS A NEW LOW END MEMBER OF THE DECSYSTEM-20 FAMILY AND FULLY SOFTWARE COMPATIBLE WITH ALL OF THE OTHER DECSYSTEM-20 MODELS.

WE INVITE YOU TO COME SEE THE 2020 AND HEAR ABOUT THE DECSYSTEM-20 FAMILY AT THE TWO PRODUCT PRESENTATIONS WE WILL BE GIVING IN CALIFORNIA THIS MONTH. THE LOCATIONS WILL BE:

TUESDAY, MAY 9, 1978 - 2 PM
HYATT HOUSE (NEAR THE L.A. AIRPORT)
LOS ANGELES, CA

THURSDAY, MAY 11, 1978 - 2 PM
DUNFEY'S ROYAL COACH
SAN MATEO, CA

Methodology that I used

- Read all of the abstracts for all of the papers in the previous 20 years of NDSS
- Sent a questionnaire to some of the key players in the network and distributed systems security and those who were involved in NDSS from the early days to get their views on how the area has changed over the past 20 years and what the future looks like
 - 75% response rate
- *What I present today is my personal opinion and not necessarily the view of the University of California nor the CIA*

Thanks to

David Balenson

Davide Balzarotti

Tom Berson

Matt Bishop

Dan Boneh

David Brumley

David Evans

Virgil Gligor

Tom Hutton

Steve Kent

Angelos Keromytis

Engin Kirda

Christopher Kruegel

Wenke Lee

Patrick McDaniel

Dan Nessel

Clifford Neuman

Hilarie Orman

Adrian Perrig

Phil Porras

Mike Reiter

William Robertson

Avi Rubin

Richard Schroepel

Radu Sion

Sal Stolfo

Dawn Song

Gene Tsudik

Paul Van Oorschot

Giovanni Vigna

Dan Wallach



Brent Waters

Who is this man?



Dan Nessel

Privacy and Security Research Group (PSRG)

- Subgroup of the Internet Research Task Force
- Became the Program Committee for 1993 NDSS Workshop
 - David Balenson 
 - Matt Bishop
 - Russell Housley
 - Steve Kent
 - John Lin
 - Dan Nessett
 - Clifford Neuman 
 - Mike Padlipsky
 - Jeff Schiller
 - Robert Shirey

Original Call for Papers

- Mostly by email
- July issue of Computer Communications review

“The goal of this workshop is to bring together individuals who have built, are building, or will soon build software and hardware concerned with the provision of network or distributed system security services . It is intended to be a forum for those interested mainly in practical aspects of network and distributed system security, rather than in theory”

11 papers in 1993

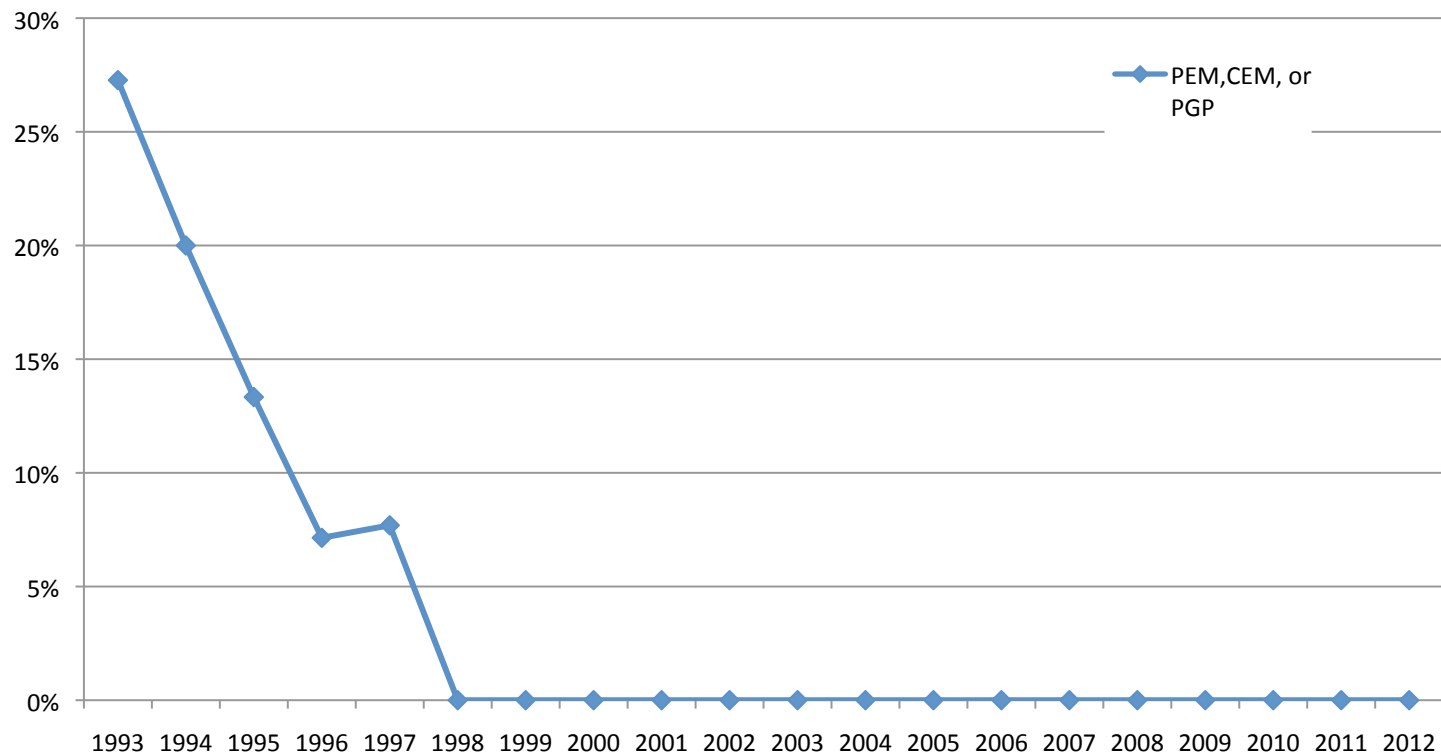
- Very practice oriented
- 3 papers on PEM
 - 1 for Unix, 1 for VMS, 1 on protecting the integrity of PEM
- 2 papers discussed large real networks
 - NREN and IT2000
- 1 distributed PKM (discussed PEM), 1 secure distributed voting, 1 distributed electronic document authorization (Workflow.2000)
- 3 distributed system security
 - practical access control, rights delegation, and secure file sharing (this one used PEM)

15 papers in 1994

- Main areas of concern were authentication, secure/private email, secure transport, and connecting to external(untrusted) networks
- 7 papers on authentication
- 3 secure/private email
- 3 Kerberos
- 2 firewall
- Lots of cryptography, certificates, and digital signatures
- Surprisingly
 - 3 talked about dial-up/telephone connections or modems
 - 2 zero-knowledge proofs

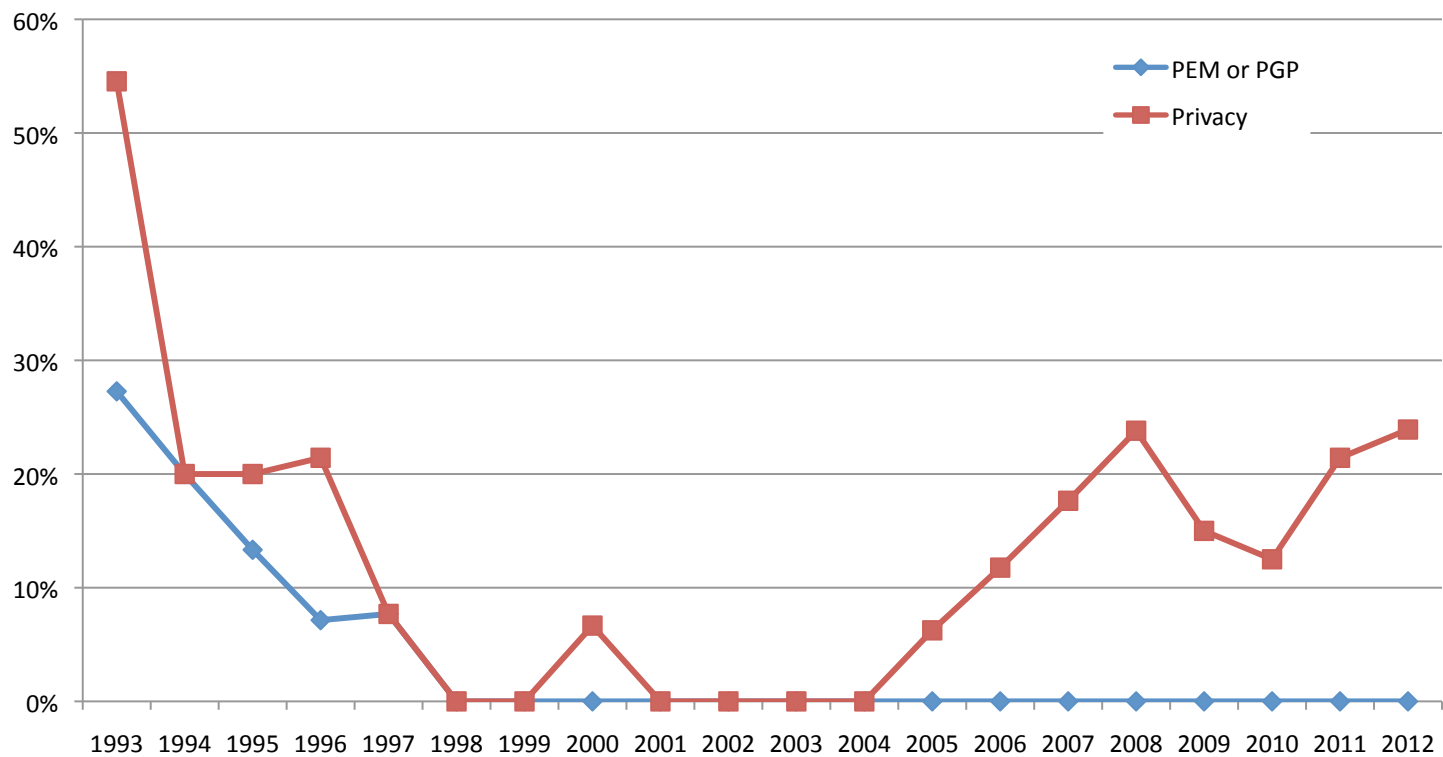
Topics

- 359 papers in the proceedings
 - 10 mention PEM, CEM, or PGP in the abstract



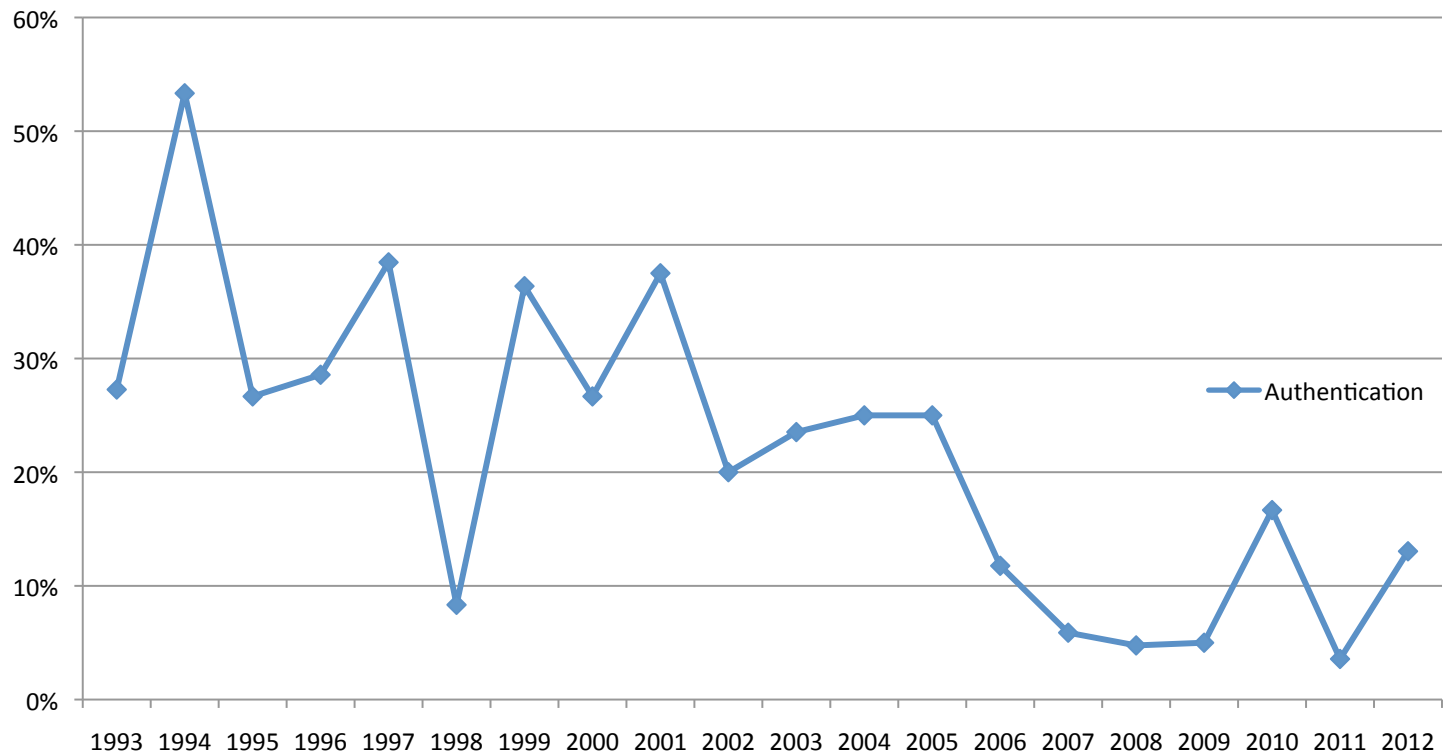
Topics

- 359 papers in the proceedings
 - 10 mention PEM, CEM, or PGP in the abstract
 - 51 mention Privacy



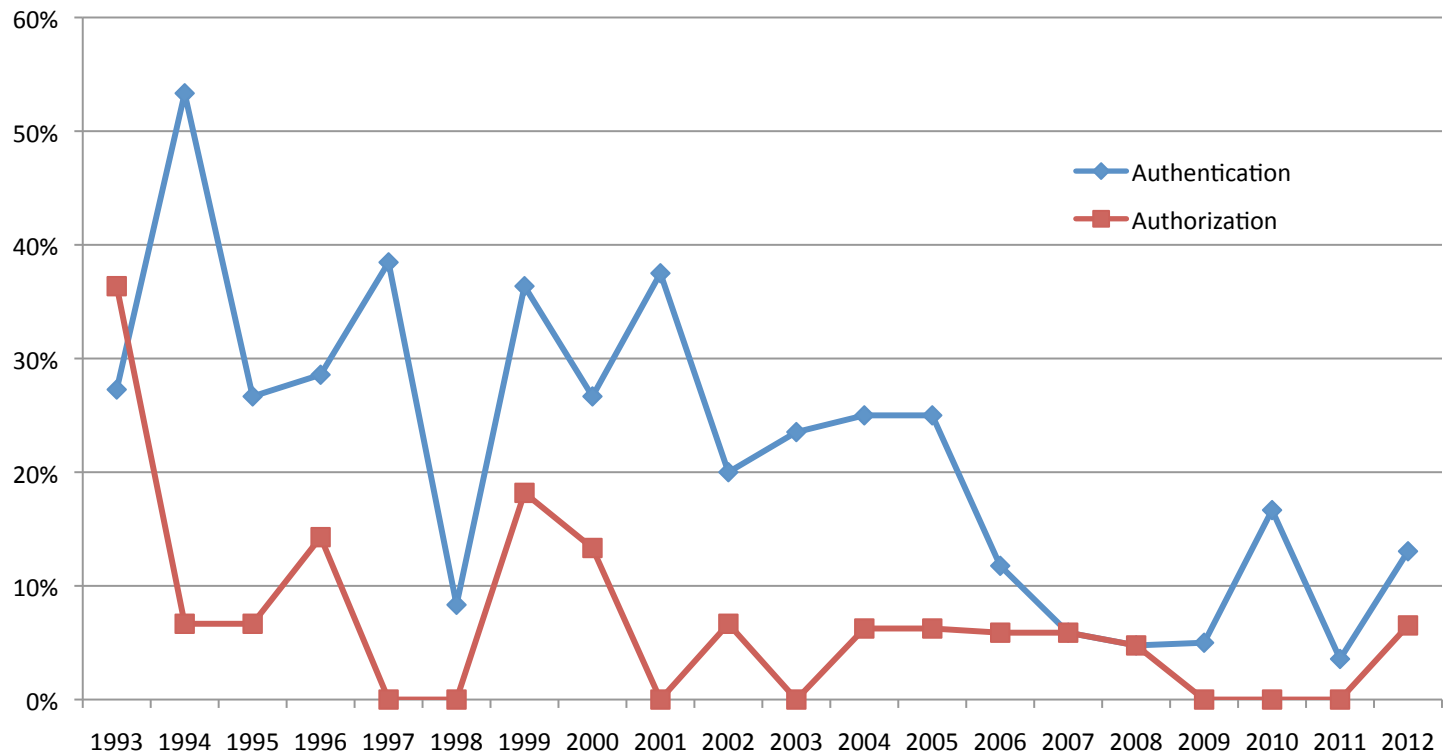
Topics

- 359 papers in the proceedings
 - 70 mention Authentication in the abstract



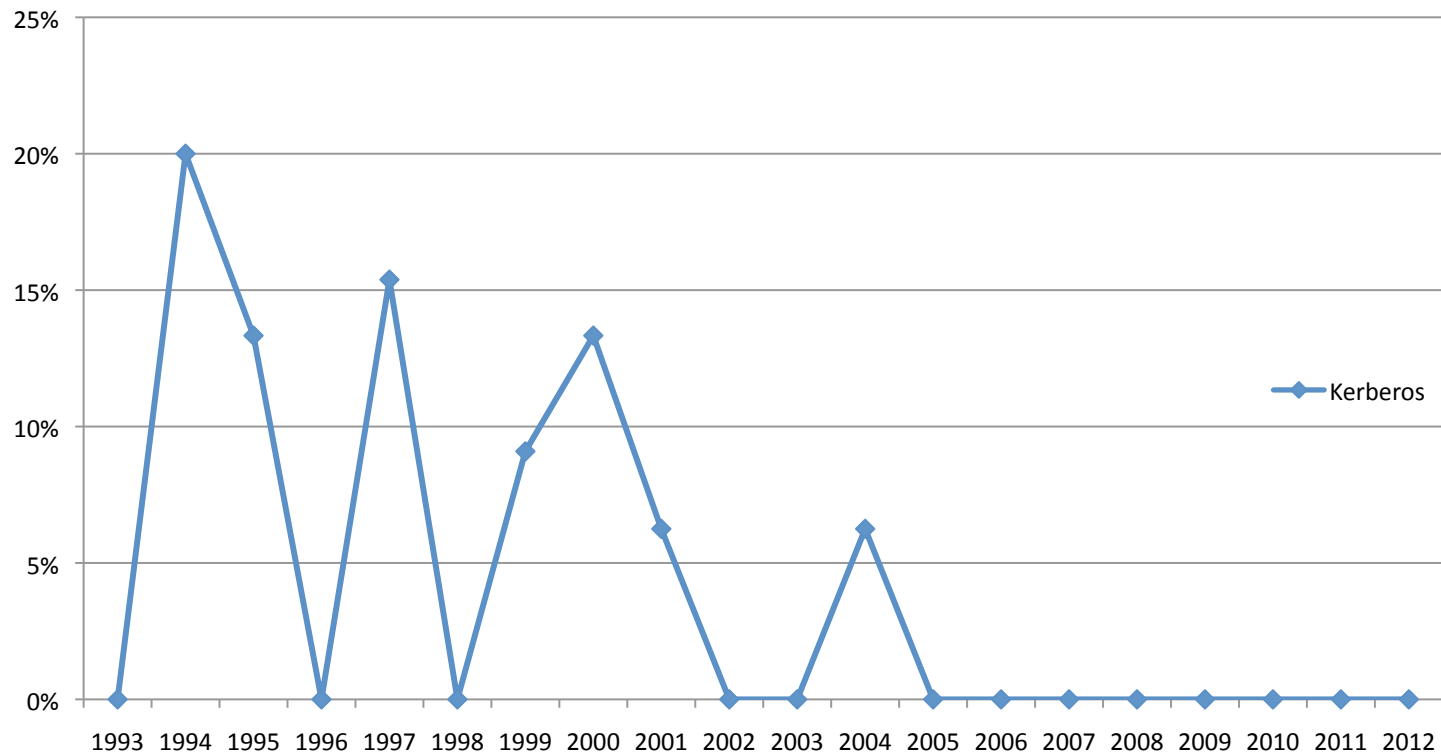
Topics

- 359 papers in the proceedings
 - 70 mention Authentication in the abstract
 - 21 mention Authorization



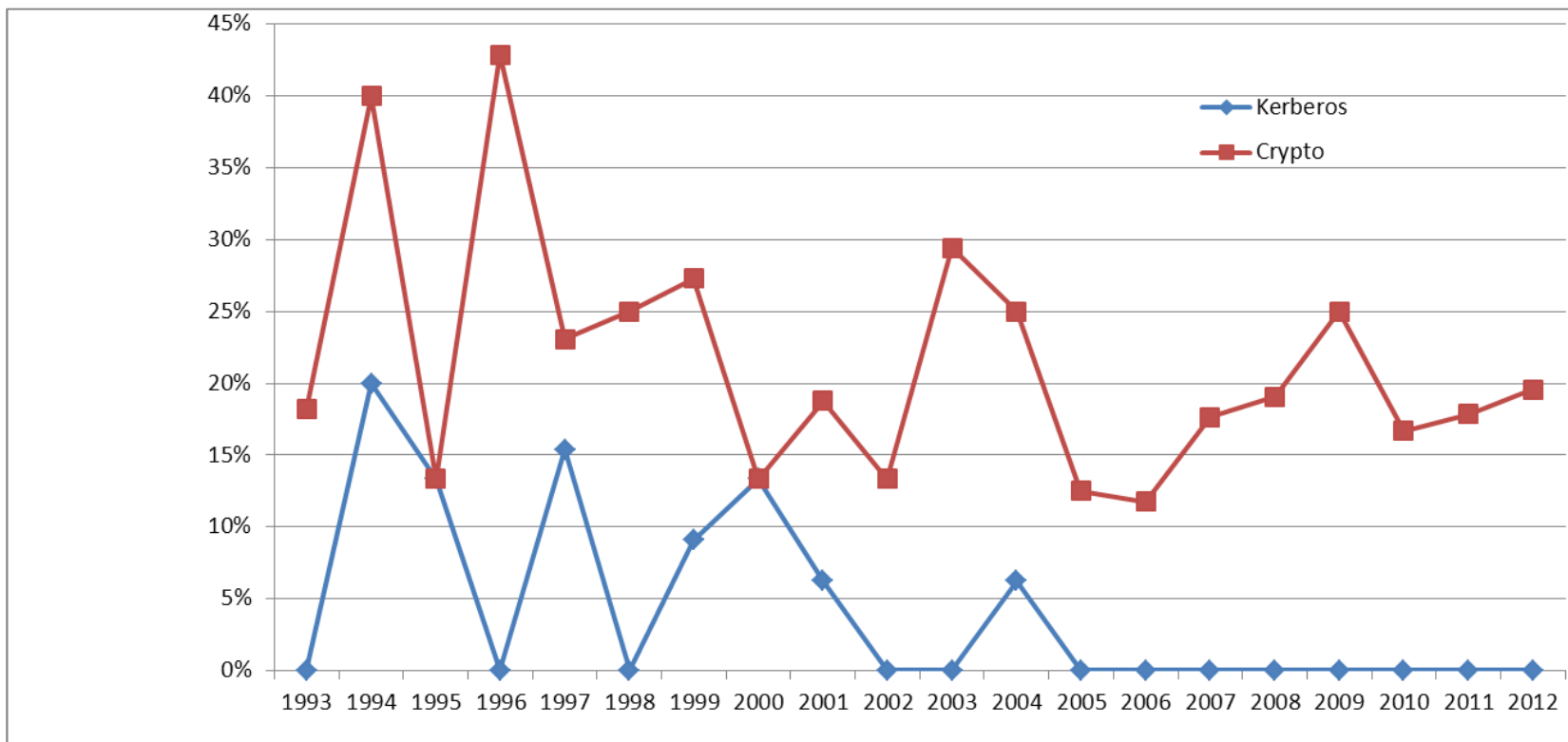
Topics

- 359 papers in the proceedings
 - 12 mention Kerberos in the abstract



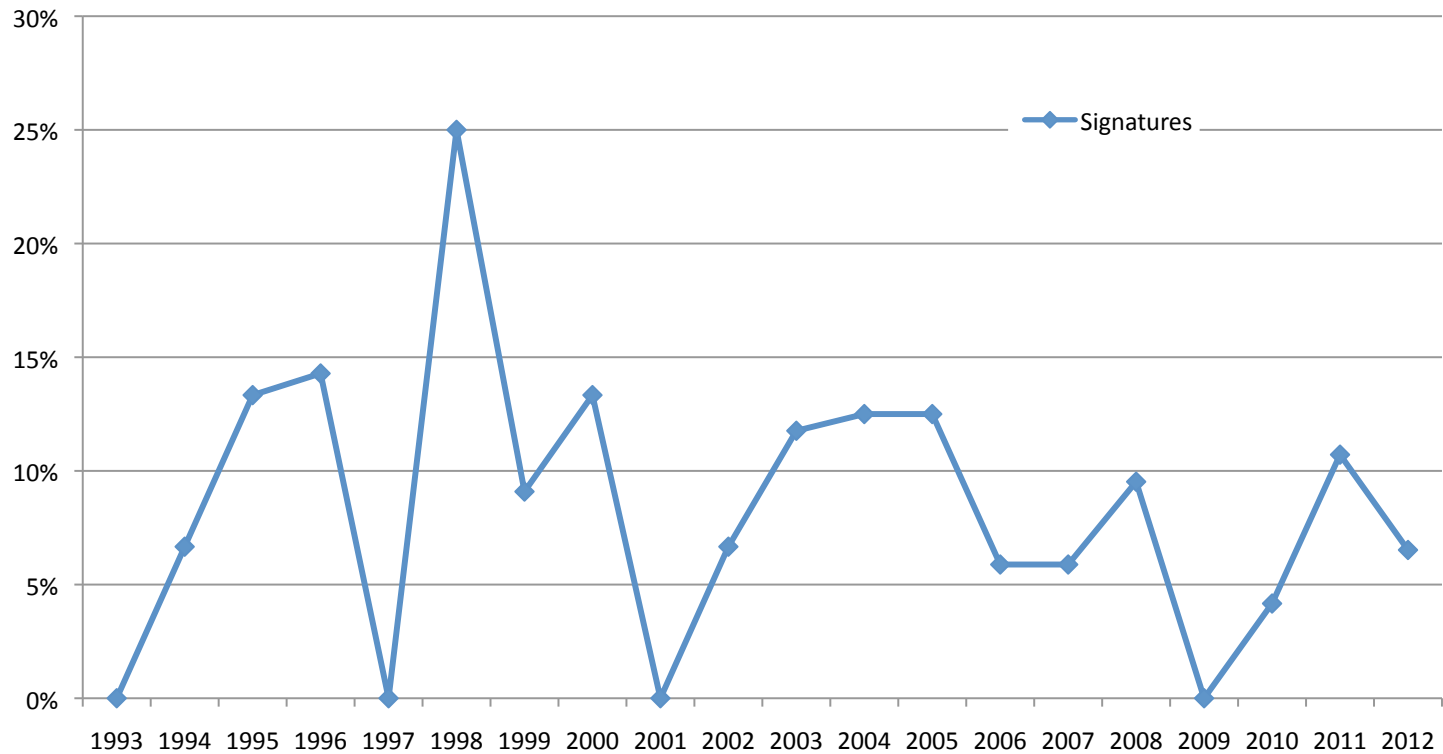
Topics

- 359 papers in the proceedings
 - 12 mention Kerberos in the abstract
 - 75 mention Crypto



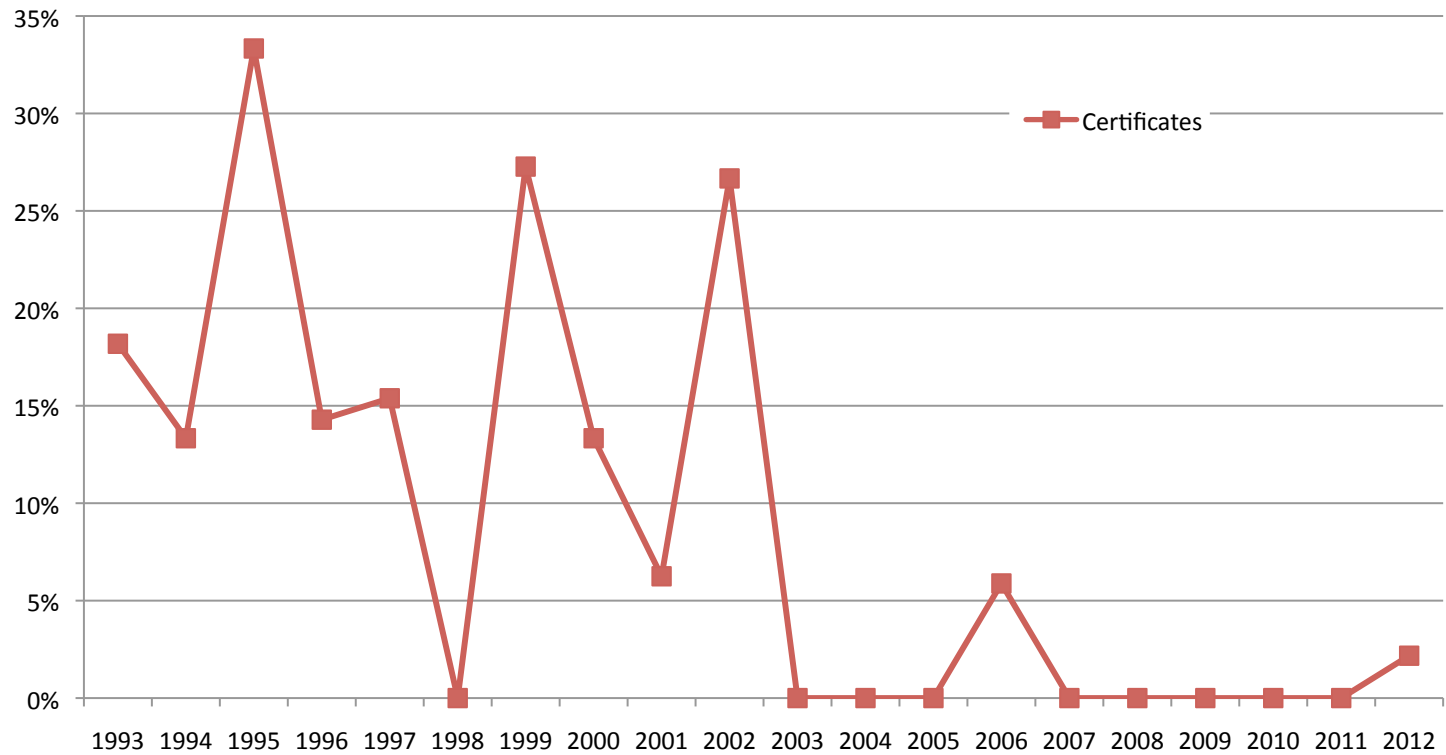
Topics

- 359 papers in the proceedings
 - 29 mention Signatures in the abstract



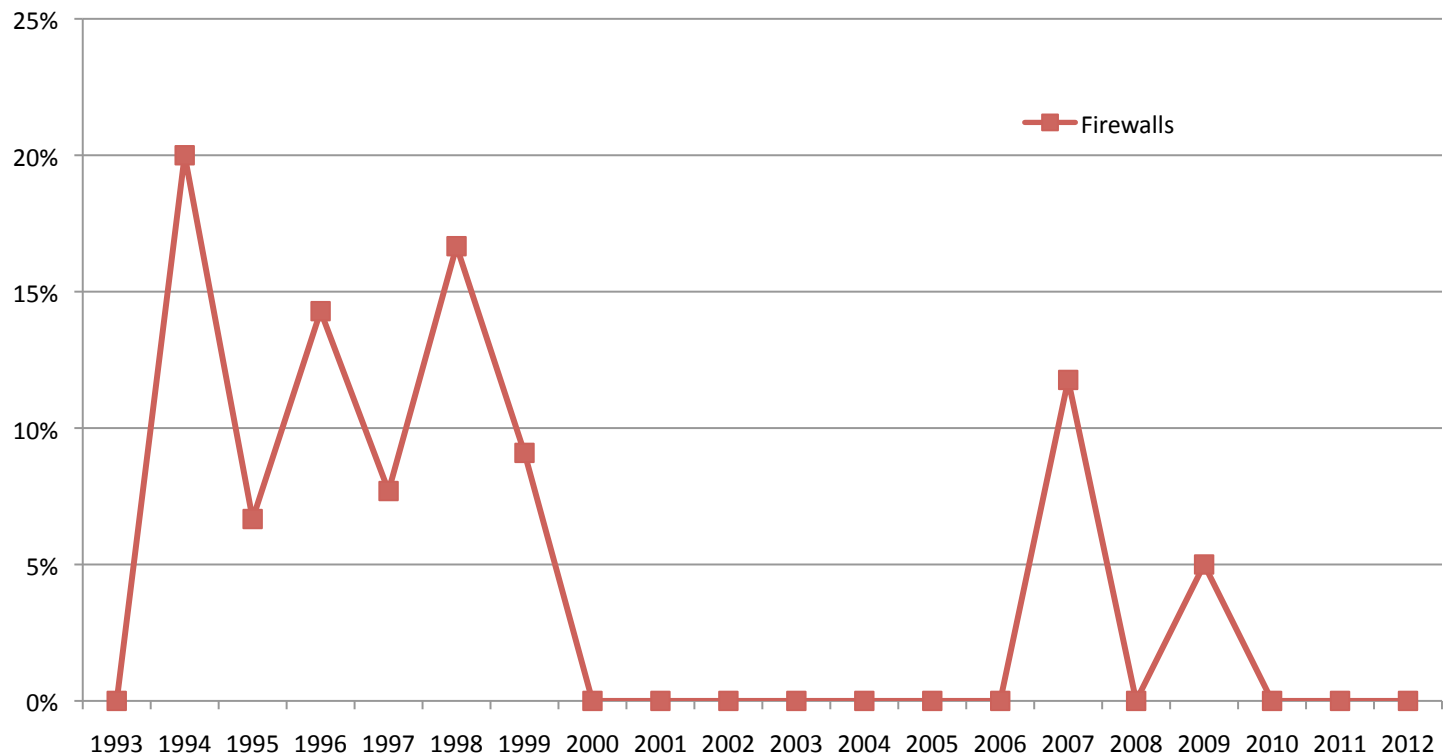
Topics

- 359 papers in the proceedings
 - 25 mention Certificates in the abstract



Topics

- 359 papers in the proceedings
 - 25 mention Firewalls in the abstract

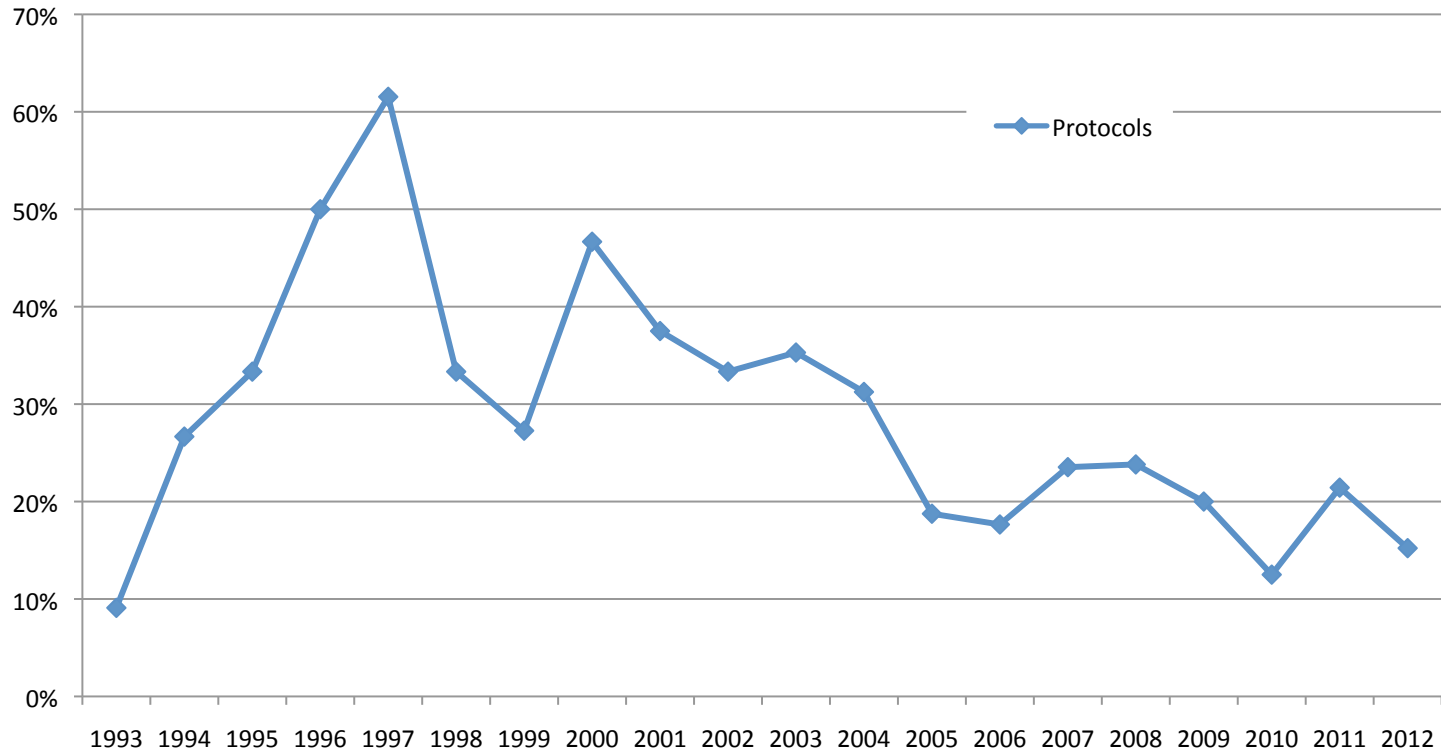


More Trends

- Protocols have always been a popular topic
 - routing, encryption, authorization, authentication, etc.
 - 60% of the papers discussed protocols in 1997

Topics

- 359 papers in the proceedings
 - 96 mention Protocols in the abstract

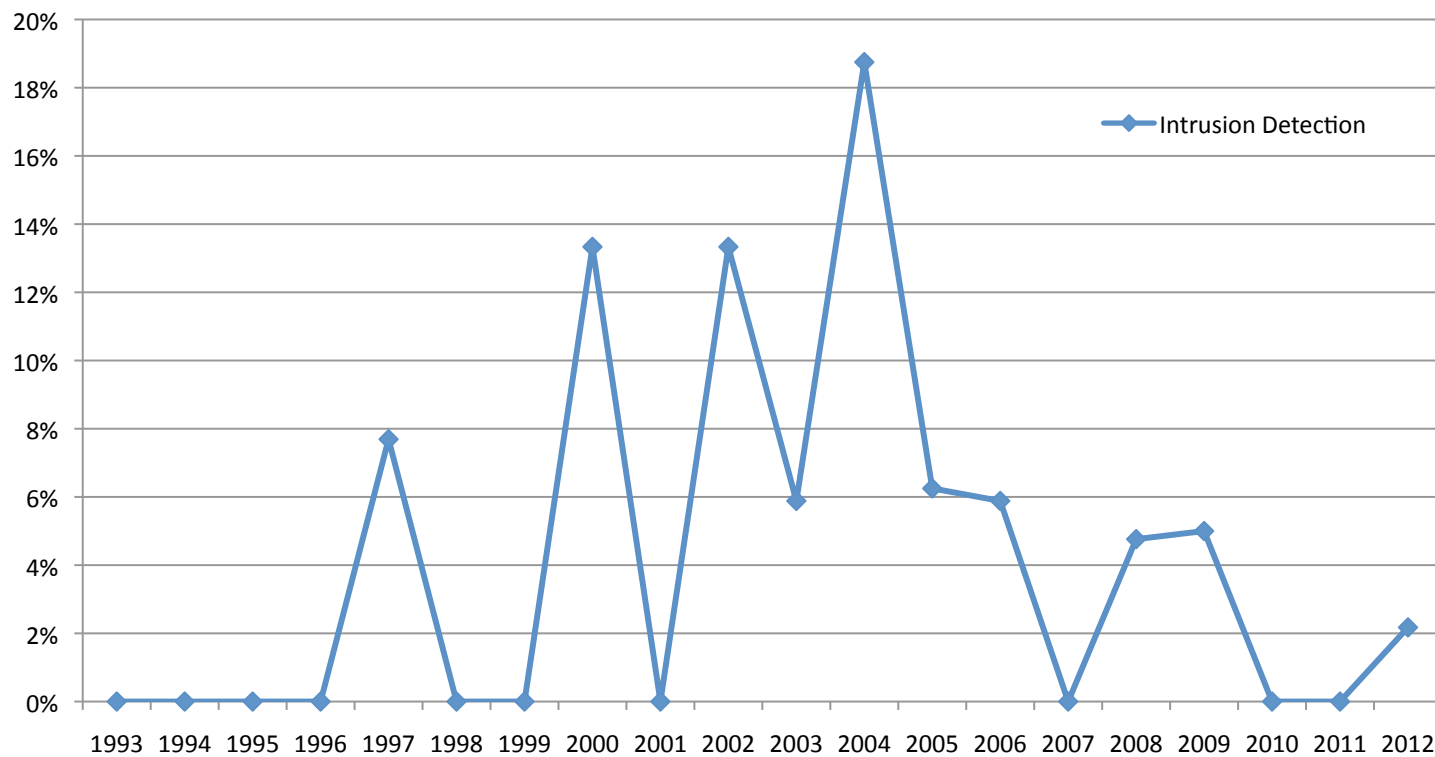


More Trends

- Intrusion Detection Systems (IDS)
 - first appeared in 1995 and they were more like network monitors
 - peaked in 2005
 - soon after it became unfashionable

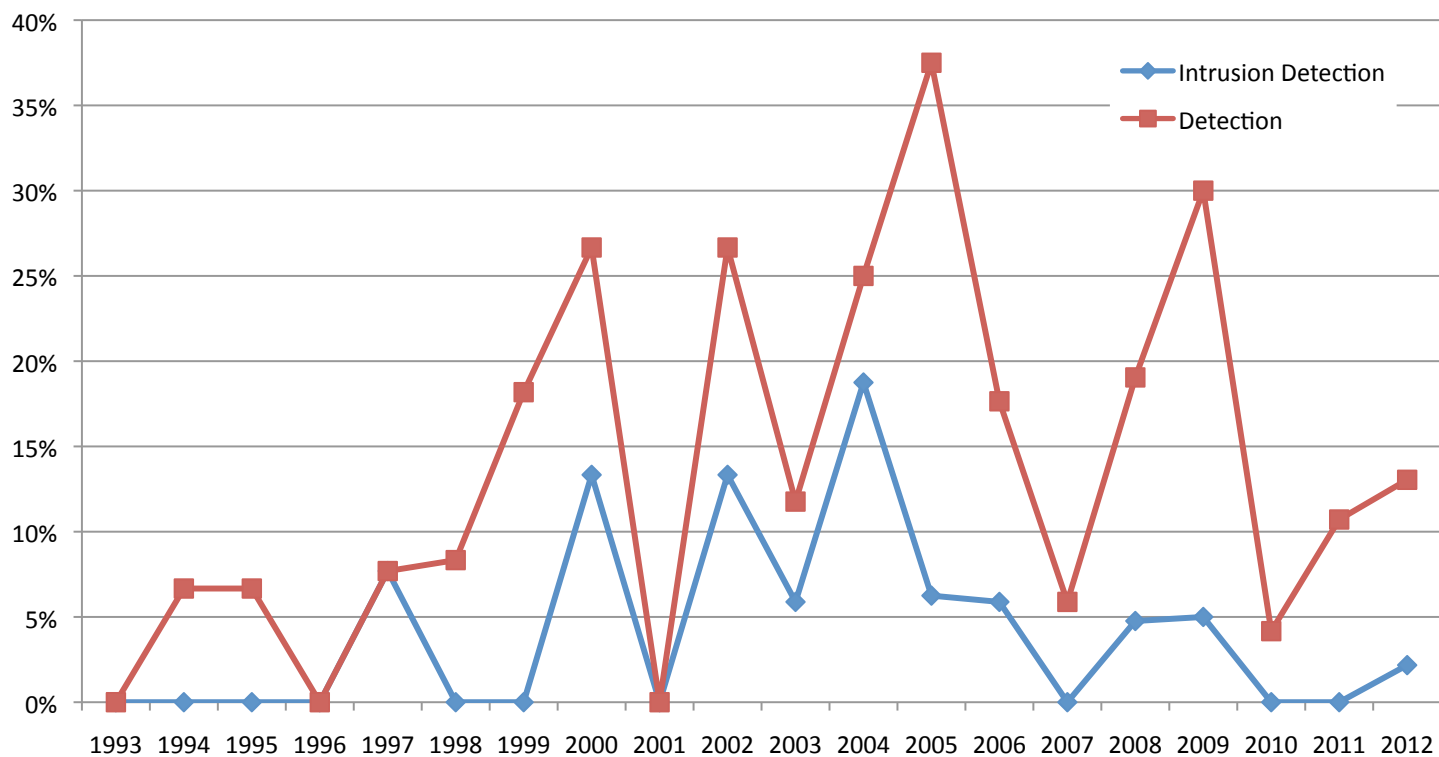
Topics

- 359 papers in the proceedings
 - 14 mention Intrusion Detection in the abstract



Topics

- 359 papers in the proceedings
 - 14 mention Intrusion Detection in the abstract
 - 50 mention Detection

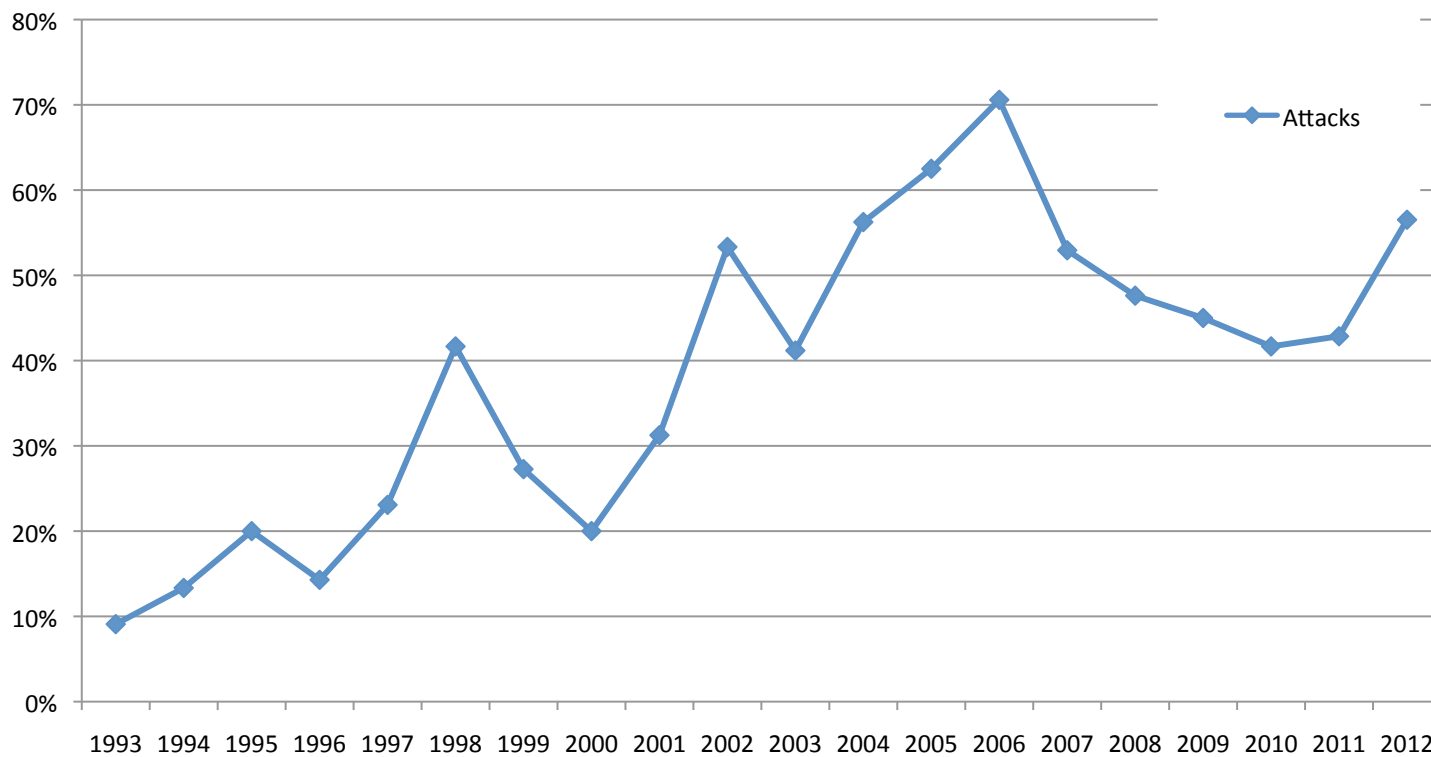


More Trends

- Attack papers really started to dominate in 1998
 - 5 of 12 papers explicitly presented a new attack
- Denial-of-Service papers started in 1999
- Spam in 2003
- Malware in 2006
- Phishing in 2007
- Still continues today

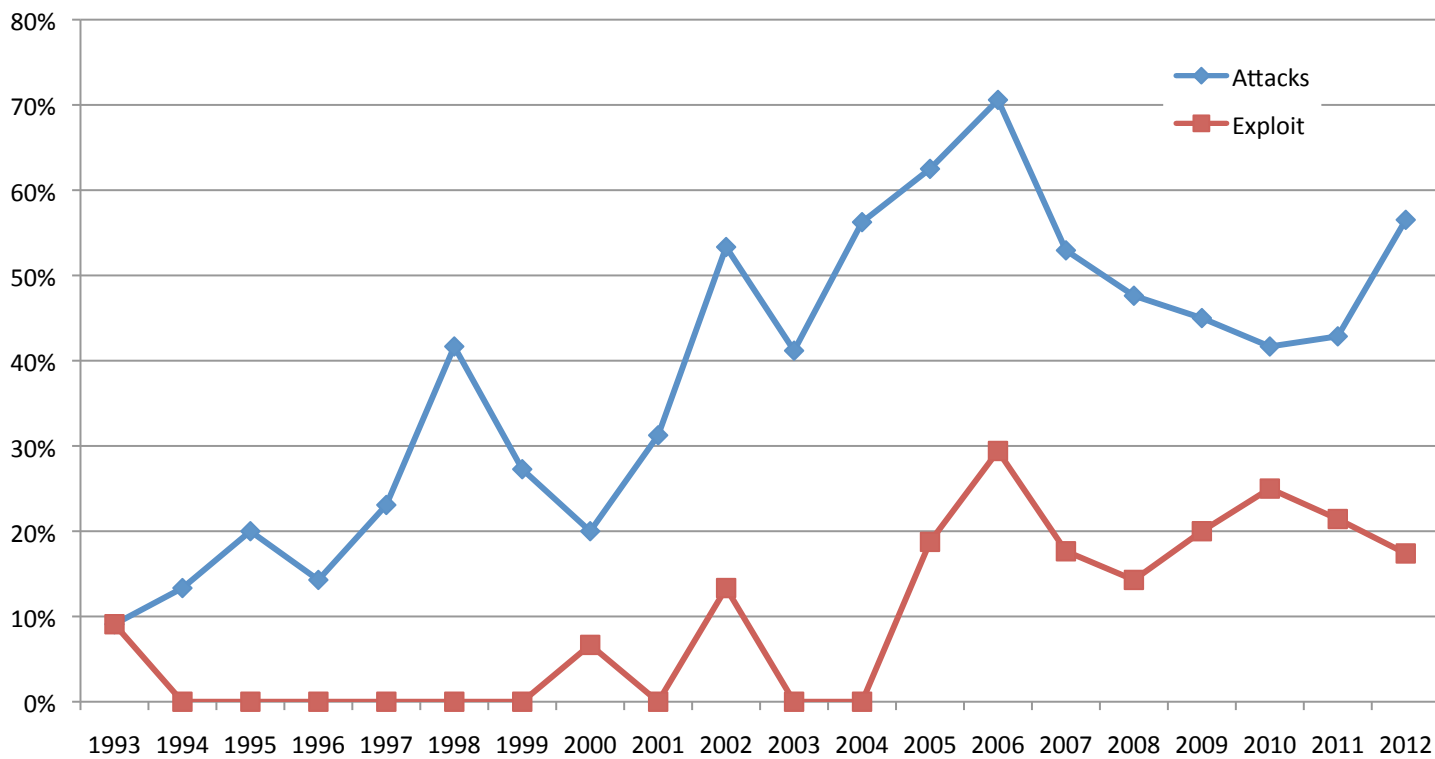
Topics

- 359 papers in the proceedings
 - 149 mention Attacks in the abstract



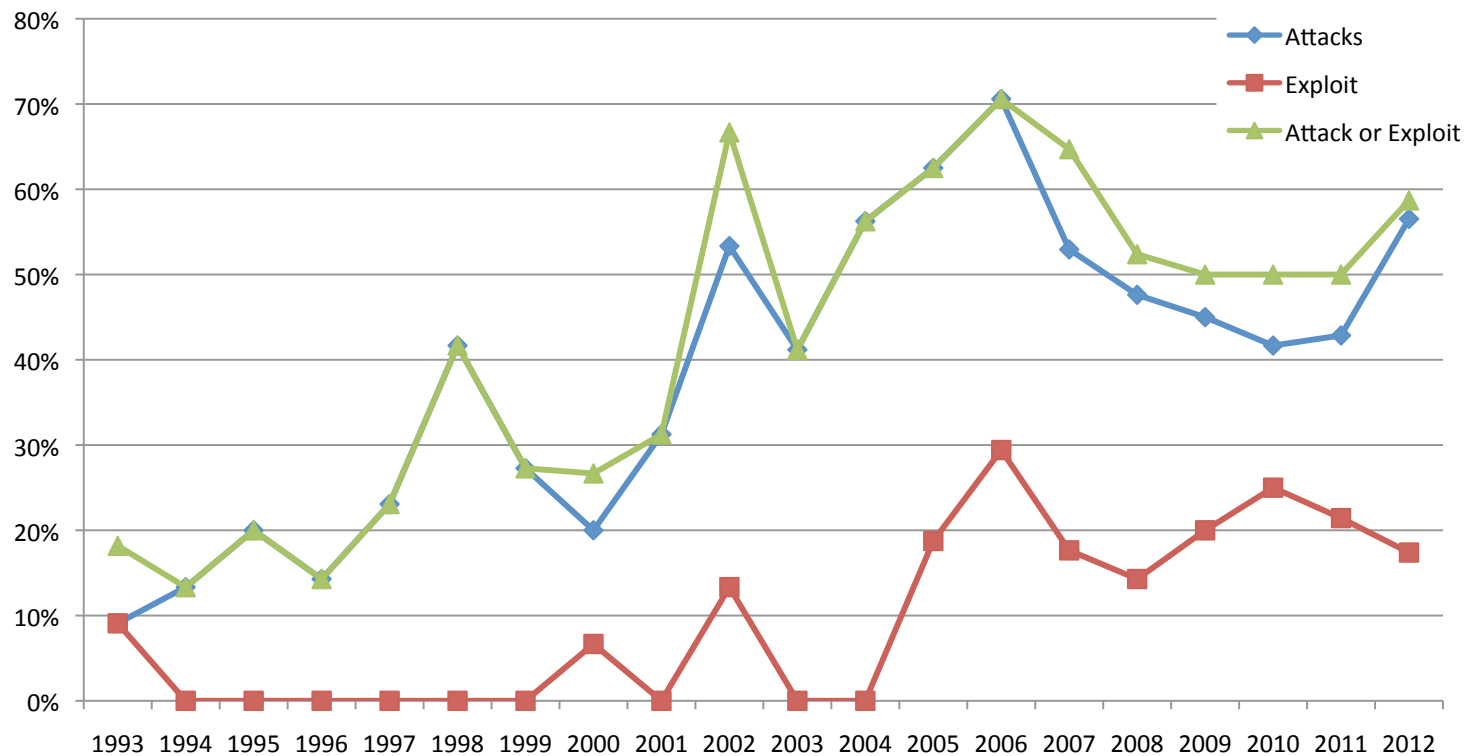
Topics

- 359 papers in the proceedings
 - 149 mention Attacks in the abstract
 - 42 mention Exploits



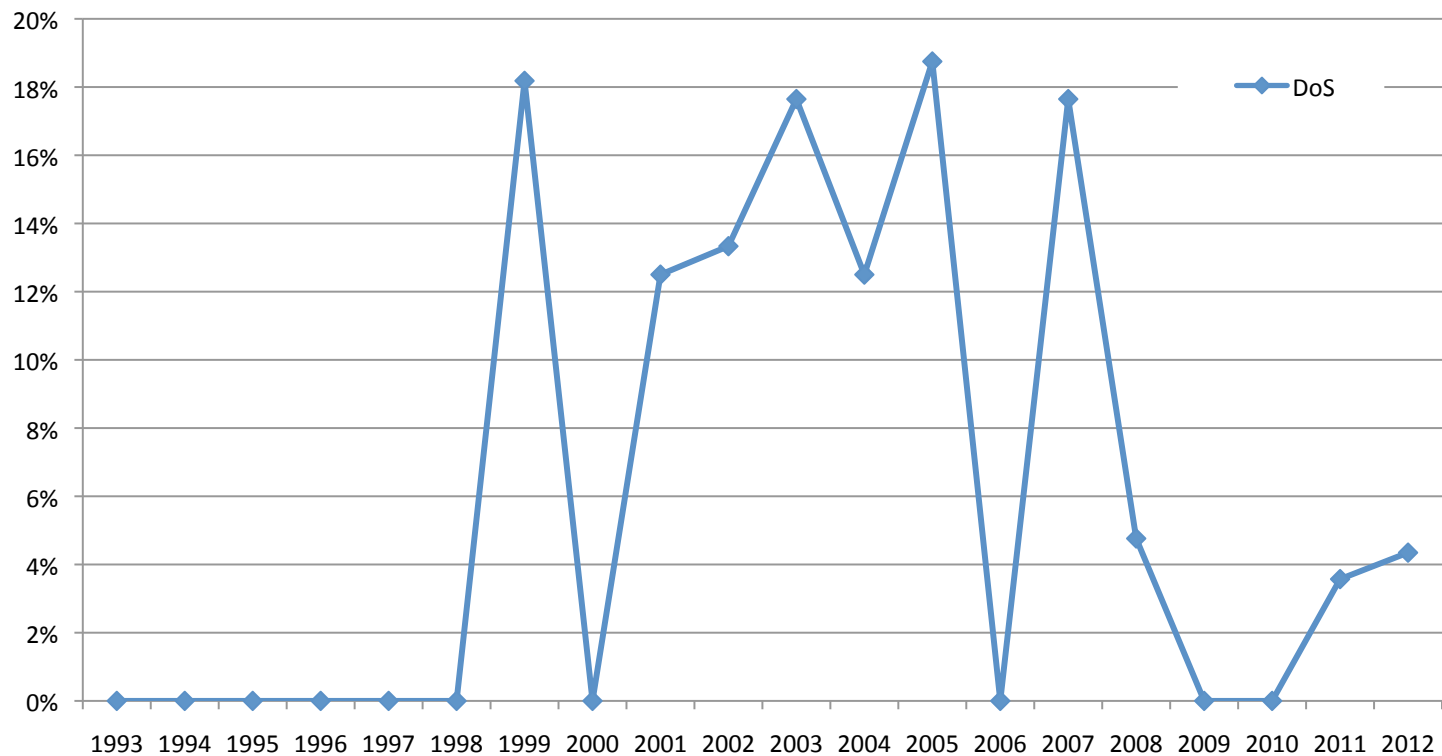
Topics

- 359 papers in the proceedings
 - 149 mention Attacks in the abstract
 - 42 mention Exploits



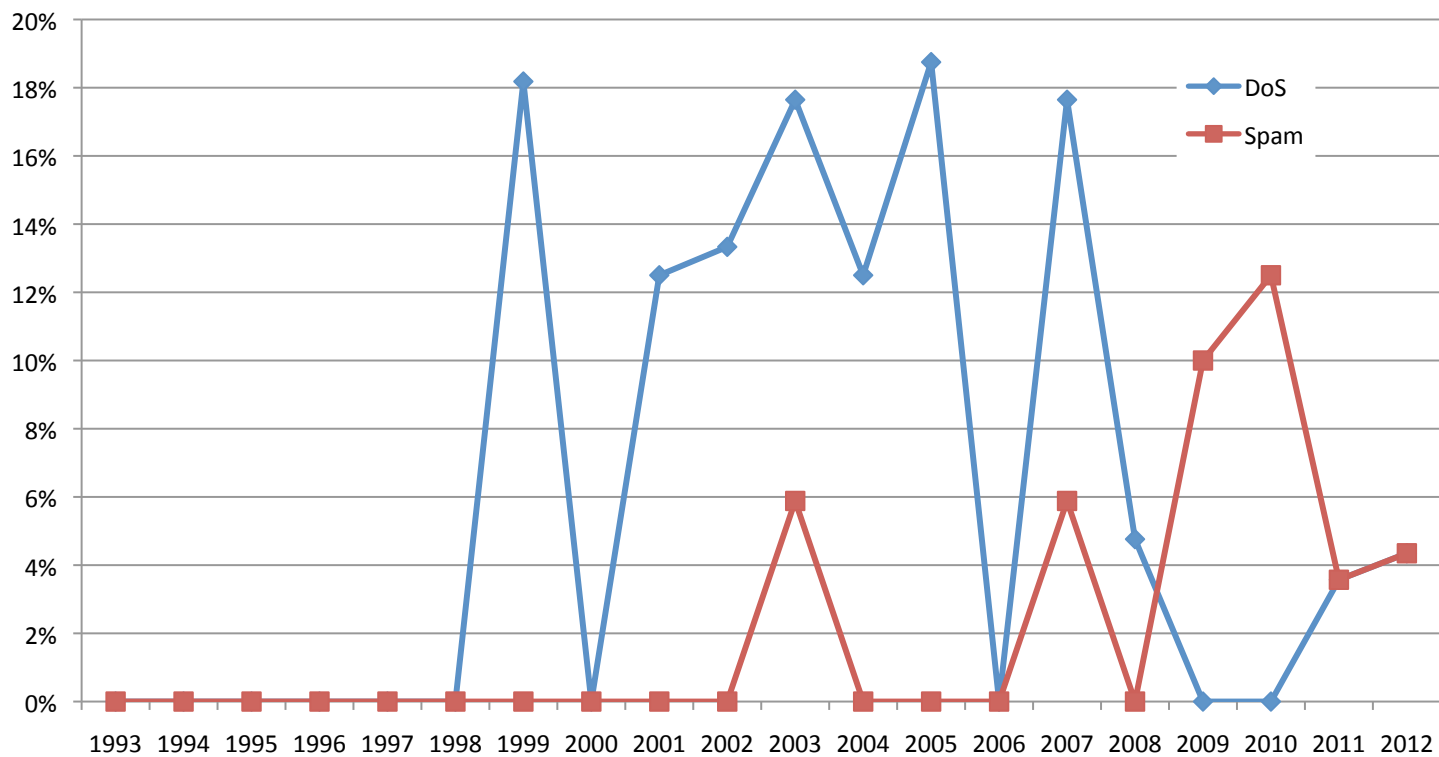
Topics

- 359 papers in the proceedings
 - 21 mention Denial-of-Service in the abstract



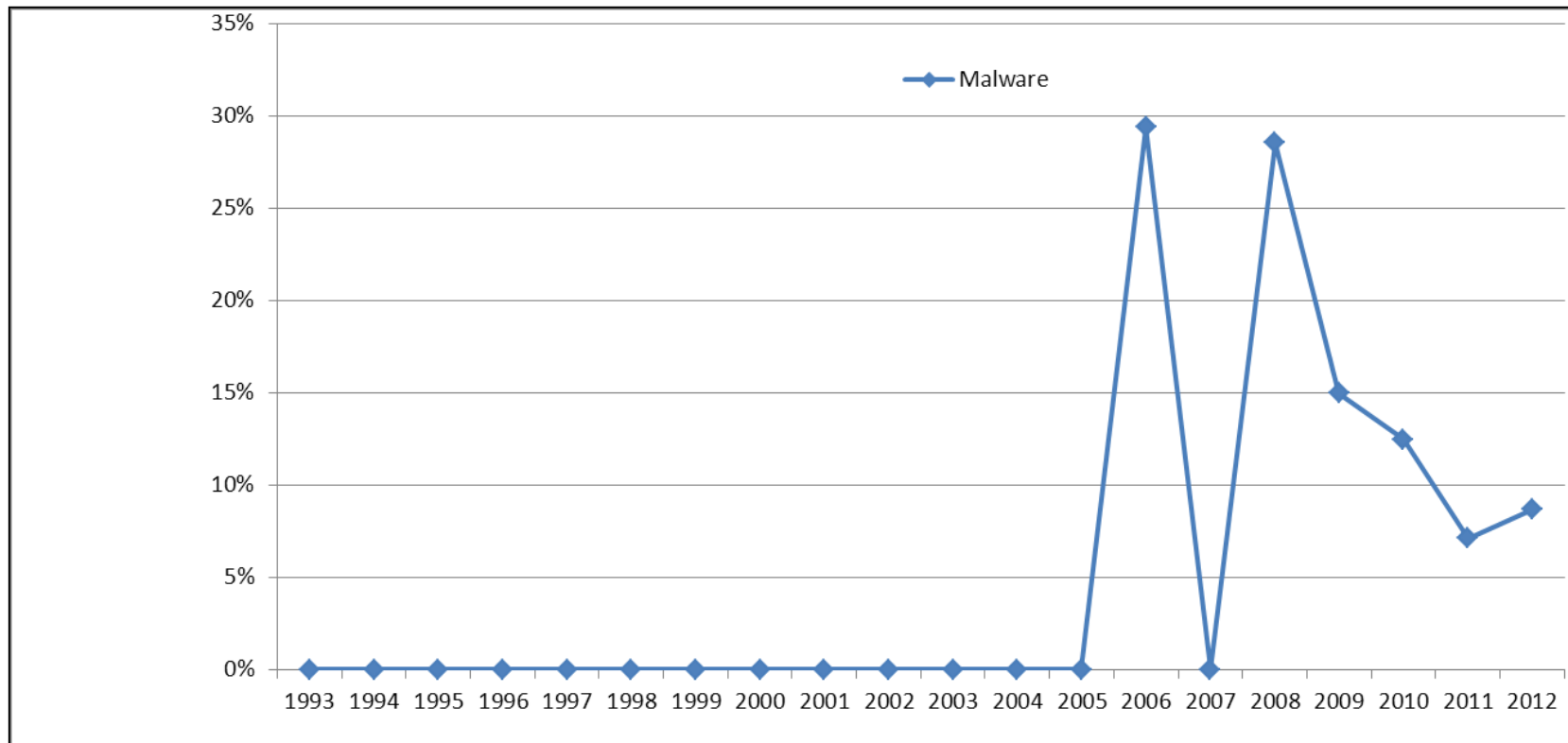
Topics

- 359 papers in the proceedings
 - 21 mention Denial-of-Service in the abstract
 - 10 mention Spam



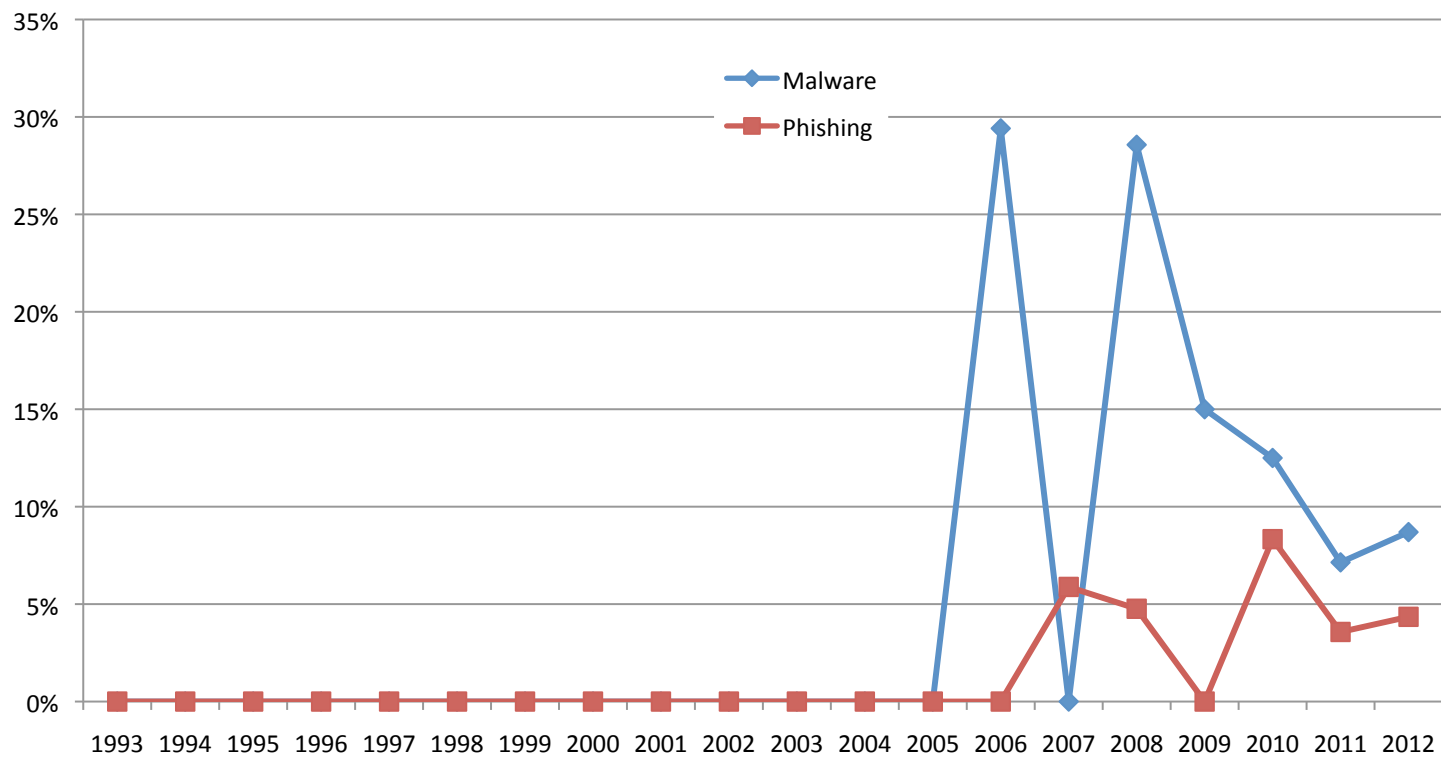
Topics

- 359 papers in the proceedings
 - 23 mention Malware in the abstract



Topics

- 359 papers in the proceedings
 - 23 mention Malware in the abstract
 - 7 mention Phishing



Last few years

- Mobile devices
- Smartphones
- Social networks
- Cloud computing
- Searchable encrypted data
- Location privacy

Overarching Trend

- The papers started becoming more general around 2003
 - operating systems
 - buffer overflows
 - language tools
- The trend continues
- Today NDSS topics are very similar to what you find at S&P, CCS, or Usenix Security
 - results in a closed publication circle

One-Off Topics

- 2 all-optical network papers in 1998

What's in a word?

- Raise your hand if you have used or recognize any of these systems/technologies:

MANIAC	PGRIP	DIRA	BotSniffer
BAfirewall	CellCase	Fig	SybilInfer
NERD	TESLA	PEAPOD	Spectogram
SNIF	TRICERT	RICH	RB-Seeker
RUSSEL	PAMINA	GAPA	K-Tracer
SESAME	SiRiUS	OPTWALL	RAINBOW
Yaksha	DOMINO	Halo	IntScope
PEMToolkit	SpoofGuard	PRECIP	CSAR
SURF	Ostia	AutoFormat	
SKEME	MOVE	HookFinder	

Future Trends

- Mobile devices, smartphones, social networks, cloud computing will continue
- More pervasive and complex systems
 - Embedded (automobile/airplane) systems/networks
 - Ubiquitous computing
- New network paradigms
 - Content-centric networking
 - Named-data networking
 - Software-defined networking
- Internet of things

Questions?



1994



1995



1996



1997



2001



2002



2003



2005



2006



2007



2008



2009



