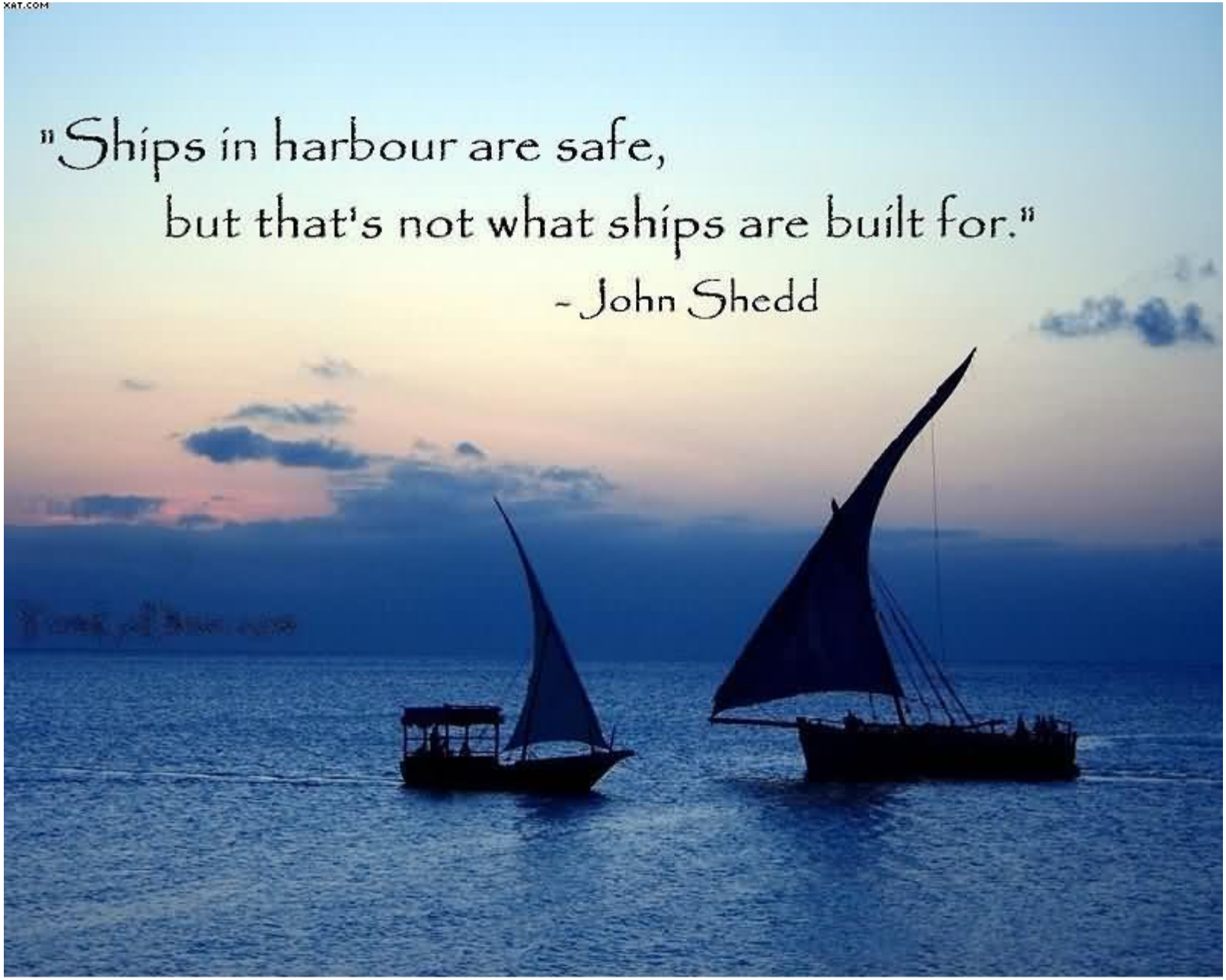
computer and network security, and the digital order

Burak Galip ASLAN, PhD


"Ships in harbour are safe,
but that's not what ships are built for."
- John Shedd

9LoLs.com

scenarios

1- Bot Roast

FBI, criminal use of botnets, operation “Bot Roast”, June 2007, 8 ppl indicted-pled guilty or sentenced for botnet activity, cooperation from overseas law enforcements, uncovering $20 million loss at more than 1 million victim computers, botnet – collection of compromised computers, remote commander – botherder, gaining control with viruses-worms and trojan horses, opening attach-clicking ad or phishing-pharming, bot computers then used for identity theft-DOS attacks, install keystroke loggers...

THE FBI FEDERAL BUREAU OF INVESTIGATION

CONTACT US | ABOUT US | MOST WANTED | NEWS | STATS

Stories

Home • News • Stories • 2007 • November • Operation Bot Roast II

'Bot Roast II'

Cracking Down on Cyber Crime

11/29/07

It's the season for online shopping and spending, and you'll be glad to know that we've stepped up our fight against one of the most serious cyber security threats just in time for the holidays.

That threat involves what are called 'botnets'—armies of personal computers taken over by cyber criminals and used on the sly to commit all kinds of mischief, from identity theft to denial of service attacks to massive spam campaigns. Bah, humbug.

In June, we announced the first phase of Operation Bot Roast, which pinpointed more than a million victimized computers and charged a number of individuals around the country with various cyber-related crimes.

scenarios

1- Bot Roast

FBI, criminal use of botnets, operation “Bot Roast”, June 2007, 8 ppl indicted-pled guilty or sentenced for botnet activity, cooperation from overseas law enforcements, uncovering $20 million loss at more than 1 million victim computers, botnet – collection of compromised computers, remote commander – botherder, gaining control with viruses-worms and trojan horses, opening attach-clicking ad or phishing-pharming, bot computers then used for identity theft-DOS attacks, install keystroke loggers... **botherders are guilty for sure but what about the users?**

scenarios

1- Bot Roast

FBI, criminal use of botnets, operation “Bot Roast”, June 2007, 8 ppl indicted-pled guilty or sentenced for botnet activity, cooperation from overseas law enforcements, uncovering $20 million loss at more than 1 million victim computers, botnet – collection of compromised computers, remote commander – botherder, gaining control with viruses-worms and trojan horses, opening attach-clicking ad or phishing-pharming, bot computers then used for identity theft-DOS attacks, install keystroke loggers... **botherders are guilty for sure but what about the users?**

- computer owners?

scenarios

1- Bot Roast

FBI, criminal use of botnets, operation “Bot Roast”, June 2007, 8 ppl indicted-pled guilty or sentenced for botnet activity, cooperation from overseas law enforcements, uncovering $20 million loss at more than 1 million victim computers, botnet – collection of compromised computers, remote commander – botherder, gaining control with viruses-worms and trojan horses, opening attach-clicking ad or phishing-pharming, bot computers then used for identity theft-DOS attacks, install keystroke loggers... **botherders are guilty for sure but what about the users?**

- computer owners? user who refuses to buy protection sw and leaves computer unprotected and vulnerable?

scenarios

1- Bot Roast

FBI, criminal use of botnets, operation “Bot Roast”, June 2007, 8 ppl indicted-pled guilty or sentenced for botnet activity, cooperation from overseas law enforcements, uncovering $20 million loss at more than 1 million victim computers, botnet – collection of compromised computers, remote commander – botherder, gaining control with viruses-worms and trojan horses, opening attach-clicking ad or phishing-pharming, bot computers then used for identity theft-DOS attacks, install keystroke loggers... **botherders are guilty for sure but what about the users?**

- computer owners? user who refuses to buy protection sw and leaves computer unprotected and vulnerable? sw devs who distribute OSs and apps that include security flaws causing vulnerability?

scenarios

2- Wiki Warfare

non-profit wikipedia foundation, volunteer collaboration based, only registered users can create new articles, <u>even anonymous users can edit existing entries</u>, some articles change day-by-day, **some change in seconds**, discussion facility for edits, wiki uses monitoring programs for obscenities and malicious activities

scenarios

2- Wiki Warfare

non-profit wikipedia foundation, volunteer collaboration based, only registered users can create new articles, <u>even anonymous users can edit existing entries</u>, some articles change day-by-day, **some change in seconds**, discussion facility for edits, wiki uses monitoring programs for obscenities and malicious activities

real event: 2008, democrats campaign, Obama vs. Clinton battle, “a candidate” – “the leading candidate” battle, “Kenyan-American and Muslim”, a volunteer contacted wiki admins and false claimers are booted, however they use false identity and come back later with other usernames

scenarios

3- Yahoo and Nazi Memorabilia

in 2000, UEJF and LICRA (French organizations), sued Yahoo in a French court that Yahoo trafficking Nazi goods in France, Yahoo initially shrugged off the suit, French law doesn't cover a US company in operating in US, French lawyer: "no permission for racism in writing, TV, radio... no reason to exclude the Internet!", Yahoo responded with "impossibility" defense, Yahoo could be held responsible for French language websites, actually French can easily visit a US website, not possible to detect where users connect, if accepted a French law becomes universal, battle raged for one country law vs. whole Internet

scenarios

3- Yahoo and Nazi Memorabilia

in 2000, UEJF and LICRA (French organizations), sued Yahoo in a French court that Yahoo trafficking Nazi goods in France, Yahoo initially shrugged off the suit, French law doesn't cover a US company in operating in US, French lawyer: "no permission for racism in writing, TV, radio... no reason to exclude the Internet!", Yahoo responded with "impossibility" defense, Yahoo could be held responsible for French language websites, actually French can easily visit a US website, not possible to detect where users connect, if accepted a French law becomes universal, battle raged for one country law vs. whole Internet

- yahoo assets in France

scenarios

3- Yahoo and Nazi Memorabilia

in 2000, UEJF and LICRA (French organizations), sued Yahoo in a French court that Yahoo trafficking Nazi goods in France, Yahoo initially shrugged off the suit, French law doesn't cover a US company in operating in US, French lawyer: "no permission for racism in writing, TV, radio... no reason to exclude the Internet!", Yahoo responded with "impossibility" defense, Yahoo could be held responsible for French language websites, actually French can easily visit a US website, not possible to detect where users connect, if accepted a French law becomes universal, battle raged for one country law vs. whole Internet

- yahoo assets in France
- new tech for location detection

scenarios

3- Yahoo and Nazi Memorabilia

in 2000, UEJF and LICRA (French organizations), sued Yahoo in a French court that Yahoo trafficking Nazi goods in France, Yahoo initially shrugged off the suit, French law doesn't cover a US company in operating in US, French lawyer: "no permission for racism in writing, TV, radio... no reason to exclude the Internet!", Yahoo responded with "impossibility" defense, Yahoo could be held responsible for French language websites, actually French can easily visit a US website, not possible to detect where users connect, if accepted a French law becomes universal, battle raged for one country law vs. whole Internet

- yahoo assets in France
- new tech for location detection
- Yahoo settled for negotiations with Chinese govn

scenarios

3- Yahoo and Nazi Memorabilia

in 2000, UEJF and LICRA (French organizations), sued Yahoo in a French court that Yahoo trafficking Nazi goods in France, Yahoo initially shrugged off the suit, French law doesn't cover a US company in operating in US, French lawyer: "no permission for racism in writing, TV, radio... no reason to exclude the Internet!", Yahoo responded with "impossibility" defense, Yahoo could be held responsible for French language websites, actually French can easily visit a US website, not possible to detect where users connect, if accepted a French law becomes universal, battle raged for one country law vs. whole Internet

- yahoo assets in France
- new tech for location detection
- Yahoo settled for negotiations with Chinese govn

Yahoo caved and removed Nazi items...

introduction

new frontier, wildwest analogy, taming... erm... civilizing the Internet ☺

sociotechnical order

Lessig (1999) argues that human behavior is regulated by

- law,

sociotechnical order

Lessig (1999) argues that human behavior is regulated by

- law,
- markets, (ISPs, email service providers)

sociotechnical order

Lessig (1999) argues that human behavior is regulated by

- law,
- markets, (ISPs, email service providers)
- social norms (emoticons, informal conventions etc.)

sociotechnical order

Lessig (1999) argues that human behavior is regulated by

- law,
- markets, (ISPs, email service providers)
- social norms (emoticons, informal conventions etc.)
- and architecture. (technological architectures – TCP/IP e.g. “specialized” pipes not available – instead “net neutrality”)

sociotechnical order

Lessig (1999) argues that human behavior is regulated by

- law,
- markets, (ISPs, email service providers)
- social norms (emoticons, informal conventions etc.)
- and architecture. (technological architectures – TCP/IP e.g. “specialized” pipes not available – instead “net neutrality”)

4 forms of regulation...

- sometimes work together, (law+architecture – bot roast)

sociotechnical order

Lessig (1999) argues that human behavior is regulated by

- law,
- markets, (ISPs, email service providers)
- social norms (emoticons, informal conventions etc.)
- and architecture. (technological architectures – TCP/IP e.g. “specialized” pipes not available – instead “net neutrality”)

4 forms of regulation...

- sometimes work together, (law+architecture – bot roast)
- sometimes clash against each other (ISP liability, legal cases ~ shaping market)

online crime

computer crimes:

1) new versions of old crimes (current law extensions)

online crime

computer crimes:

1) new versions of old crimes (current law extensions)

2) crimes that couldn’t exist w/o computers or are directed at computers (new law requirements)

online crime

computer crimes:

1) new versions of old crimes (current law extensions)

2) crimes that couldn’t exist w/o computers or are directed at computers (new law requirements) --- bank robbery?

online crime

computer crimes:

1) new versions of old crimes (current law extensions)

2) crimes that couldn't exist w/o computers or are directed at computers (new law requirements) --- bank robbery?

A- bank robbery physically (a physical risk)

online crime

computer crimes:

1) new versions of old crimes (current law extensions)

2) crimes that couldn't exist w/o computers or are directed at computers (new law requirements) --- bank robbery?

A- bank robbery physically (a physical risk)

B- bank robbery with computer (no physical risk)

online crime

computer crimes:

1) new versions of old crimes (current law extensions)

2) crimes that couldn't exist w/o computers or are directed at computers (new law requirements) --- bank robbery?

A- bank robbery physically (a physical risk)

B- bank robbery with computer (no physical risk)

"B is a new version of A" doesn't help much in moral evaluation

online crime

<u>conceptualizing new behavior is needed</u> for deciding whether a new law is needed or not. (phishing vs. offline fraud – face2face or non-delivery fraud etc.)

analogy equivalence isn't that important, "moral equivalence" should be considered

most common crime on Internet was Internet auction fraud 44,9% as of 2007

online crime as of 2019

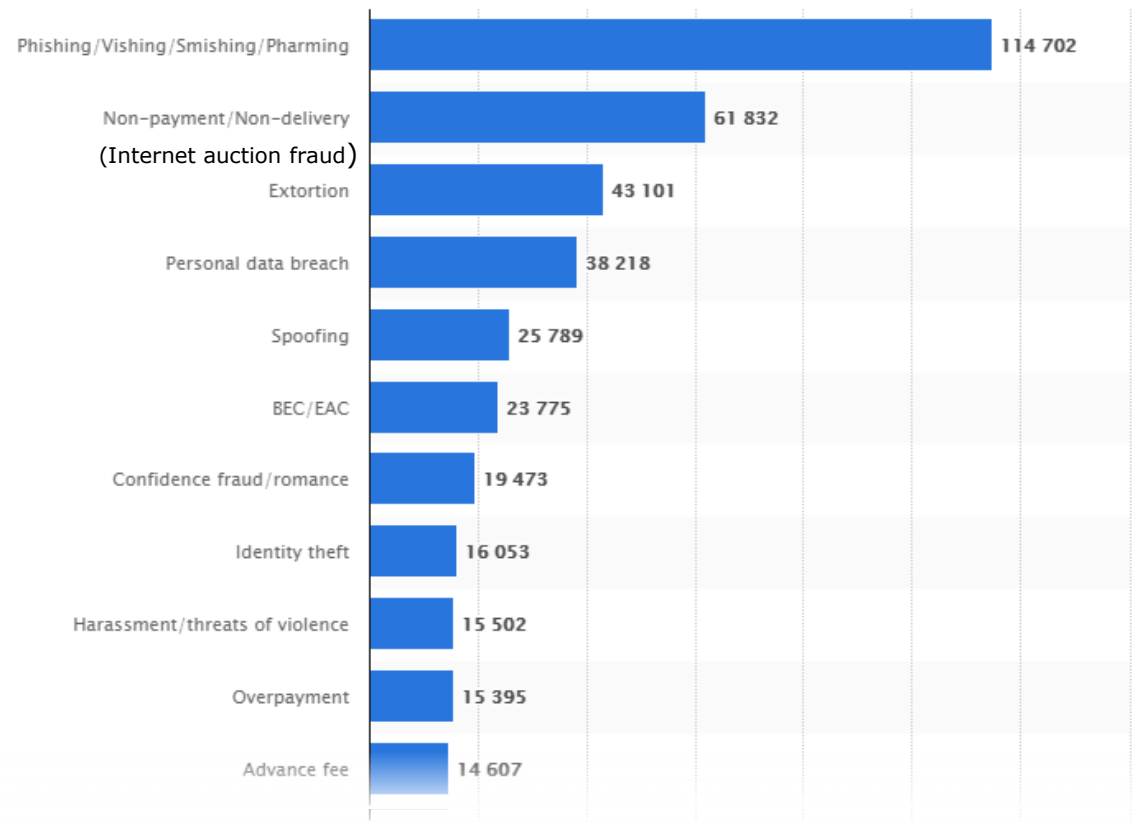
statista

Search Statistics

Prices & Access | Statistics | Reports | Outlooks | Tools | Infographics | Services | Global Survey NEW

Internet › Cyber Crime

Types of cyber crime most frequently reported to the IC3 in 2019, by victim count



DOWNLOAD

PDF + XLS + PNG

Sources

→ Show sources information

→ Show publisher information

Release date

February 2020

Region

Worldwide

Survey time period

2019

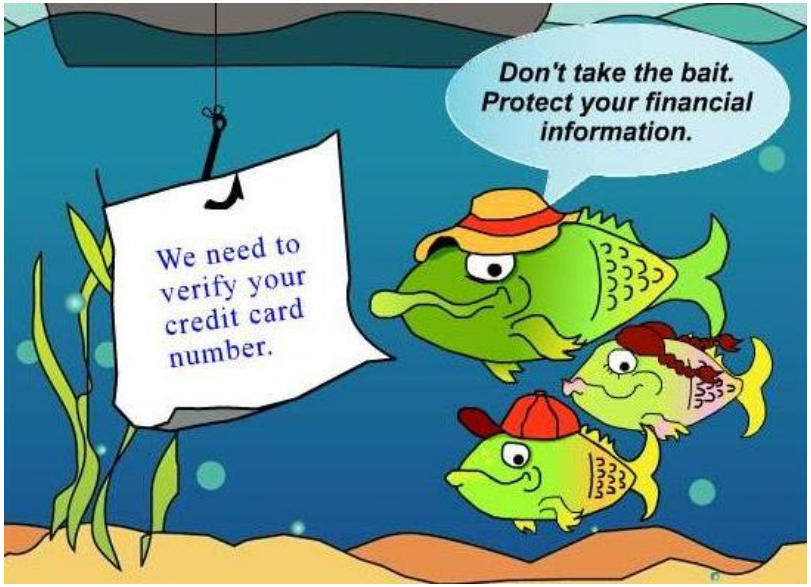
Special properties

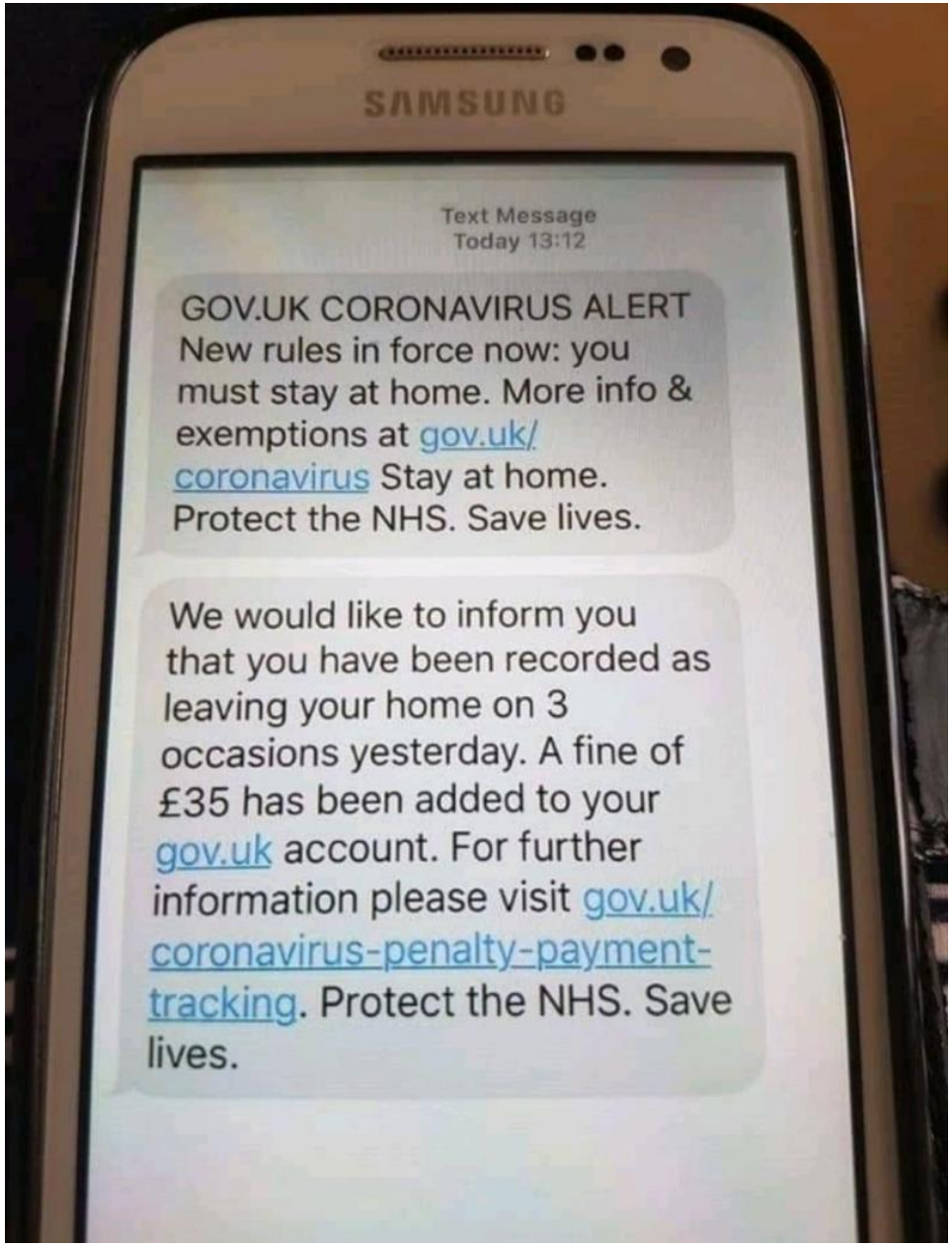
crimes reported to IC3

Supplementary notes

In 2019, the United States accounted fc
approximately 20 percent of complaint

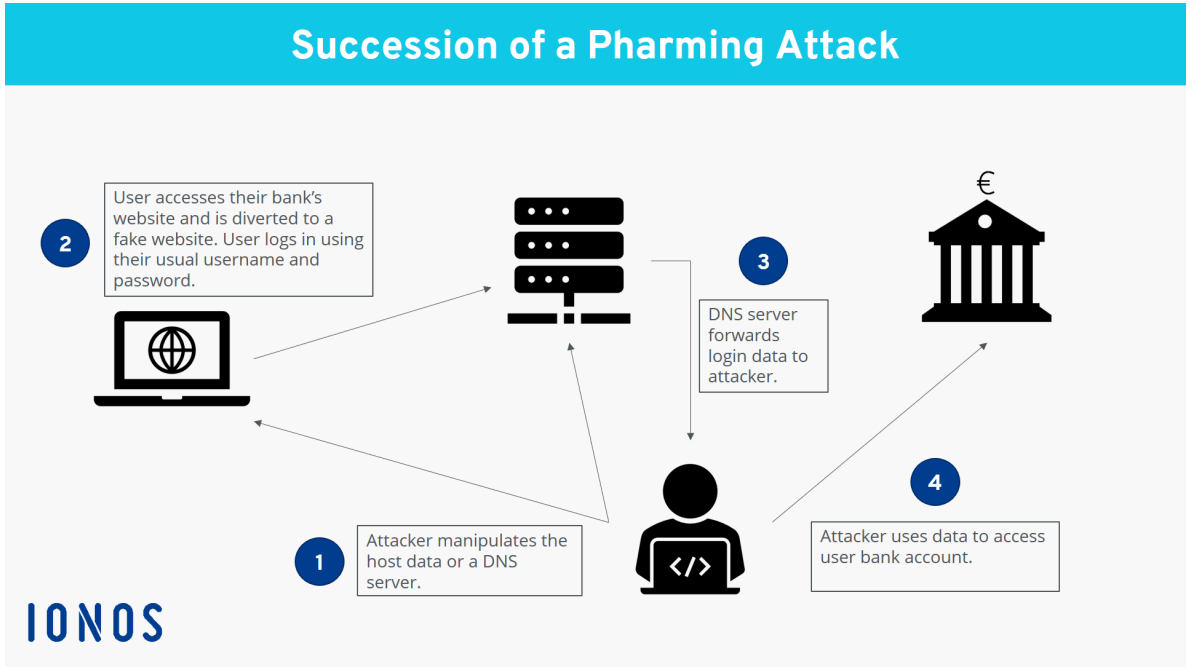
phishing, vishing, smishing





pharming

phishing without a lure



Once you visit a certain website, a DNS cache forms so you don't have to visit the server each time you return to the site. Both the DNS cache and the DNS server can be corrupted by pharming. This can result in two types of pharming.

pharming

malware-based pharming on host data

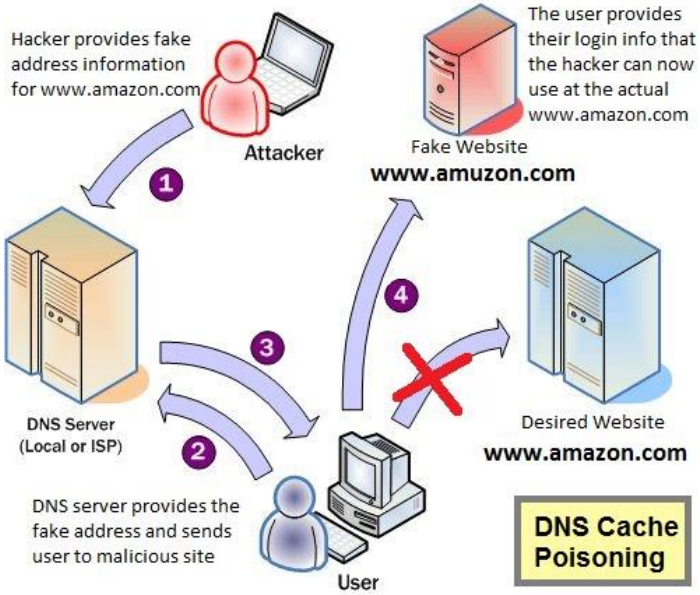
In this case, you may pick up a Trojan or virus via a malicious email or download. The malware then covertly reroutes you to a fake site created and controlled by fraudsters when you type in your intended website address.

In this form of pharming, malicious code sent in an email etc. can change your computer’s local host files. These corrupted host files can then direct your computer to fraudulent sites regardless of the Internet address you type.

pharming

DNS server poisoning

Domain Name Systems are computers on the Internet that direct your website request to the right IP address. A rogue, corrupted DNS server, however, can direct network traffic to an alternate, fake IP address.



This pharming scam doesn’t rely on corrupting individual files, but rather occurs at the DNS server level by exploiting a vulnerability. The DNS table is essentially poisoned, so you’re being redirected to fraudulent websites without your knowledge.

If a large DNS server is corrupted, cybercriminals could target and scam an even larger group of victims.

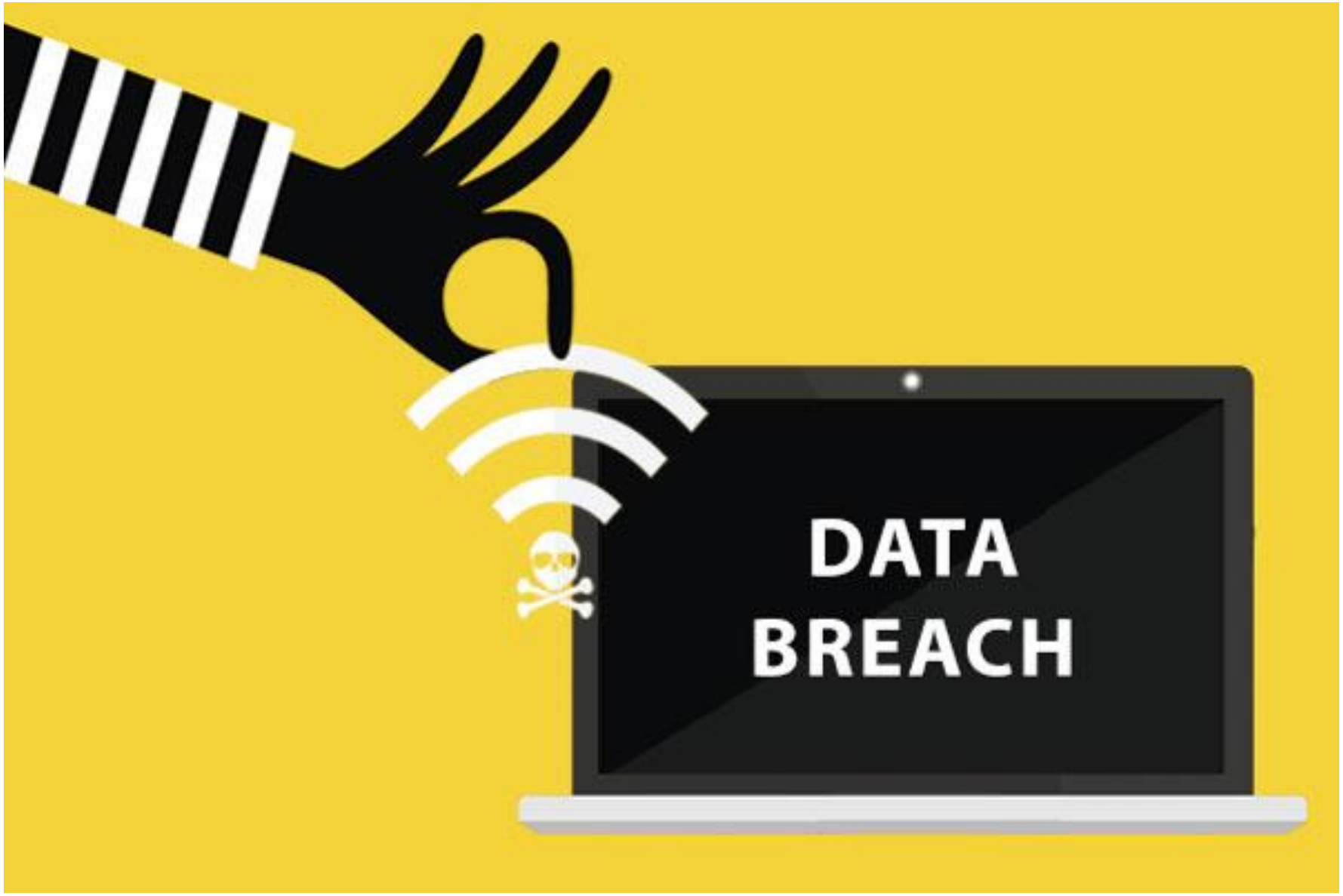
non-payment / non-delivery

INTERNET AUCTION FRAUD

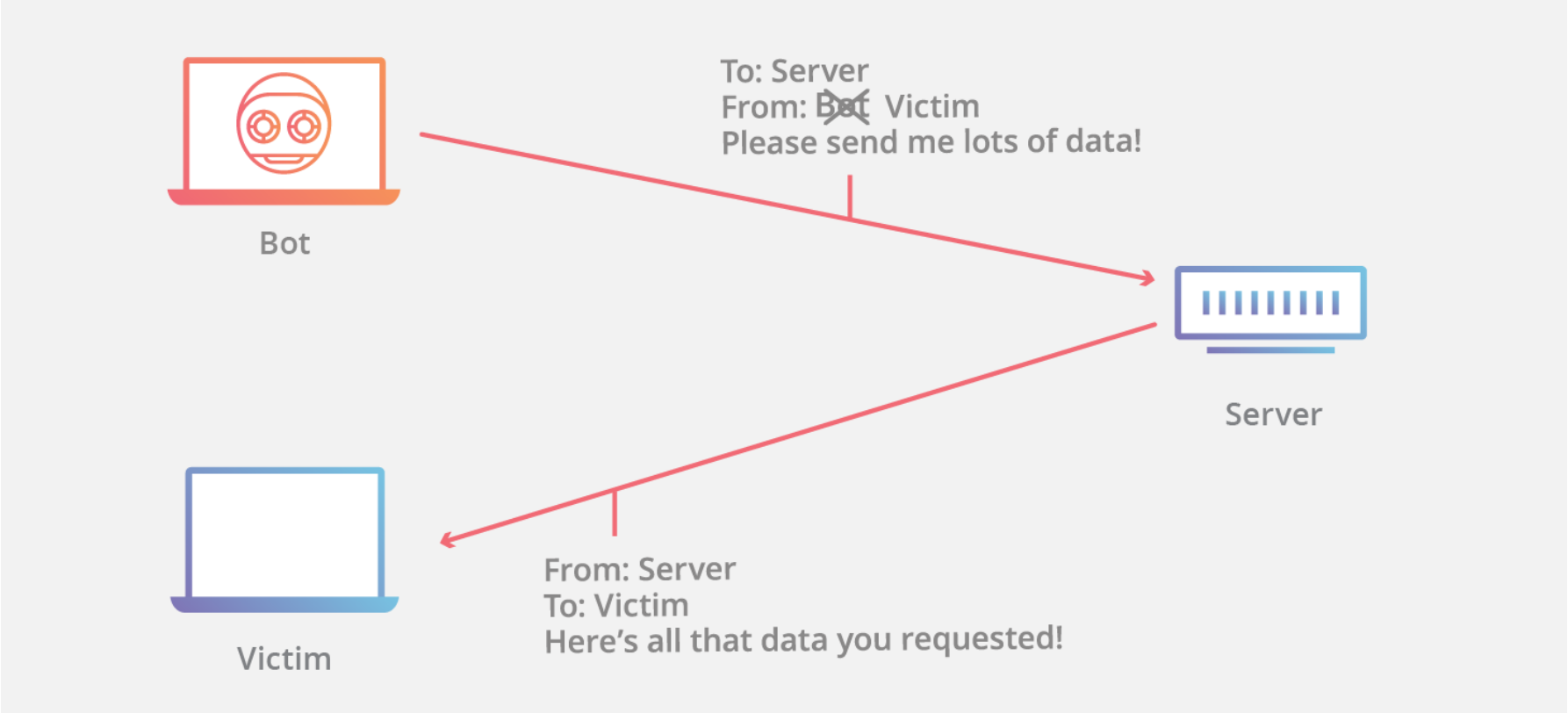
- Buyers making a payment and not receiving the merchandise or receiving merchandise that is of poor quality.
- Sellers not receiving payment for their merchandise
- Drive up the bidding price: Bid Shilling or Bid Shielding

ransomware, (s)extortion -> blackmail

personal data breach



spoofing


To: Server
From: ~~Bot~~ Victim
Please send me lots of data!
Bot
Server
Victim
From: Server
To: Victim
Here's all that data you requested!

BEC / EAC


How to Shield Your Company
From BEC Attacks
PHISHME
Business Email Compromise/Email Account Compromise (BEC/EAC) scams can destroy businesses.
2,370%
Increase in financial losses from BEC/EAC 1
$5.3 Billion USD
in actual and attempted loses from BEC/EAC 2
131 Countries
Impacted by BEC/EAC scams 3

confidence fraud / romance

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

August 05, 2019

Alert Number
I-080519-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field

CYBER ACTORS USE ONLINE DATING SITES TO CONDUCT CONFIDENCE/ROMANCE FRAUD AND RECRUIT MONEY MULES

WHAT IS CONFIDENCE/ROMANCE FRAUD?

Confidence/romance fraud occurs when an actor deceives a victim into believing they have a trust relationship—whether family, friendly, or romantic—and leverages the relationship to persuade the victim to send money, provide personal and financial information, or purchase items of value for the actor. In some cases, the victim is persuaded to launder money on behalf of the actor.

Actors often use online dating sites to pose as U.S. citizens located in a foreign country, U.S. military members deployed overseas, or U.S. business owners seeking assistance with lucrative investments.

THREAT

In 2017, more than 15,000 people filed complaints with the FBI's Internet Crime Complaint Center (IC3) alleging they were victims of confidence/romance fraud and reporting losses of more than $211 million. In 2018, the number of victims filing these complaints increased to more than 18,000, with more than $362 million in losses—an increase of more than 70 percent over the previous year.

identity theft

- **Phishing** occurs when cybercriminals senc
  trick you into opening attachments or click
  information. If you want to visit, say, your b
- **Pharming** occurs when your browser, comp
  into the address bar, but you're redirected t
  type into the website.
- **Malicious software.** Fraudsters may try to
  your PII. Consider purchasing online securi
  up to date.
- **Unsecure websites.** Avoid online shopping
  Make sure you use only official, secure web
- **Weak passwords** used for both social and
  for each of your accounts. And when possi
  credentials *and* a secret code sent to your
- **Discarded computers and mobile devices**
- **Targeting children online.** Kids can give aw

overpayment

Hello Mr. (edited by Roadfly to protect identity),

Good to hear from you and thanks for the mail,my client who said he's interested in your vehicle has promised to be buying it and will be issuing a certified cashier's cheque of $32,500 and you deduct the amount of your vehicle which is $24,000 after which you will send the difference $8,500 via Money Gram money transfer to my P.A here in Europe to settle our shipper to book us for their cargo and also pay for the insurance, she would be comming over to your place to pick the vehicle up and get it transported to the Europe and also to sign all require documents.

To bring to your attention,it only takes (24HRS) for a certified cashier's cheque to get cash in the US,so I will like you to get the cheque cashed the same day it's presented on the counter and I will also like to know if I can count on you to send the difference of the money to my P.A as soon as the cheque get to you and verified.To make things fast and coovenient for the both of us,I will like you to give me the exact name you want on the check.....Your mailing address....(Street,City,State and zip code) and your Phone # so I can forward it to my associate,so he could start with the procurement of the cheque and won't mind to engage in a long lasting bussiness relationship.

Thanks and hope to hear from you soon.

Best Regard,

Madida

advance fee

2. (c) Nigerian Advanced Fee Fraud (4-1-9)

From: "Mr. Don Peter" To: undisclosed-recipients:;
Subject: Dear Friend
Date: Thu, 18 Oct 2007 08:39:10 -0400
Reply-to: hellen_doris1@yahoo.fr

Dear Friend

It has been long we communicate last, am so sorry for the delay, I want to Inform you that your cheque of ($850.000.00) Which my boss asked me to mail to you as soon as you requested it, is still with me.

But due to some minure issue you fails to respond at the Approprete time, and presently the cheque is with me here in LAGOS-NIGERIA Though i had a new contact from a friend of mine who works with one security company here in NIGETIA that will deliver you your cheque at your door step with a cheeper rate, which the company said that it will cost you the sum of $198.00 usd, So you have to Contact them and register with them now.

online crime

distinctiveness of IT again: global, many-to-many scope, special identity conditions, reproducibility issues…

hackers and hacker ethic

at first “hacking” -> doing clever things with tech. that never been done before, usually young men, BB sharing knowledge, computer clubs, user groups

FOSS movement is an evolution and extension of this community

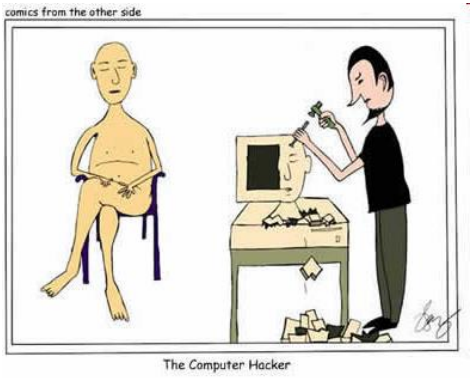
hackers and hacker ethic

at first “hacking” -> doing clever things with tech. that never been done before, usually young men, BB sharing knowledge, computer clubs, user groups

FOSS movement is an evolution and extension of this community

later hacker ~ illegality, where in fact “cracker”

however distinction didn’t hold and “hacker” became common



hackers defense

1)“all information should be free”

public libraries accesibility for all, if democratic society as many as possible well-informed citizens, info on marketplace -> uneven distribution undermining equality and democracy

hackers argue that too much info is being proprietary, they saw the enormous potential of Internet for info distribution

hackers defense

1)“all information should be free”

public libraries accesibility for all, if democratic society as many as possible well-informed citizens, info on marketplace -> uneven distribution undermining equality and democracy

hackers argue that too much info is being proprietary, they saw the enormous potential of Internet for info distribution

counter: all free info -> no market -> no incentive to develop info... + no need to keep personal info (privacy?)

hackers defense

1)“all information should be free”

public libraries accesibility for all, if democratic society as many as possible well-informed citizens, info on marketplace -> uneven distribution undermining equality and democracy

hackers argue that too much info is being proprietary, they saw the enormous potential of Internet for info distribution

counter: all free info -> no market -> no incentive to develop info... + no need to keep personal info (privacy?)

+argument: “certain kinds” of info should be free...

hackers defense

1)“all information should be free”

public libraries accesibility for all, if democratic society as many as possible well-informed citizens, info on marketplace -> uneven distribution undermining equality and democracy

hackers argue that too much info is being proprietary, they saw the enormous potential of Internet for info distribution

counter: all free info -> no market -> no incentive to develop info... + no need to keep personal info (privacy?)

+argument: “certain kinds” of info should be free... how to distinguish that “certain”?

hackers defense

2) “hackers often break into systems beneficially to point out security problems.” i.e. no stealing or damage

hackers defense

2) “hackers often break into systems beneficially to point out security problems.” i.e. no stealing or damage

counter: Gene Spafford (1992), Spafford’s powerful analogy, continual break ins to homes to reveal weakly secured houses O_o?

hard to justify whistle-blowing for such cases

hackers defense

3) “break-in but ok as long as no harm or <u>no change</u>, learning about computer systems, no loss at all”

hackers defense

3) “break-in but ok as long as no harm or <u>no change</u>, learning about computer systems, no loss at all”

violation of privacy

hackers defense

3) “break-in but ok as long as no harm or <u>no change</u>, learning about computer systems, no loss at all”

violation of privacy

also even access can cause “physical harm” e.g. slowing down computer systems at hospitals etc. -> at least stealing CPU cycles

hackers defense

3) “break-in but ok as long as no harm or <u>no change</u>, learning about computer systems, no loss at all”

violation of privacy

also even access can cause “physical harm” e.g. slowing down computer systems at hospitals etc. -> at least stealing CPU cycles

you can learn a lot by hacking but learning isn’t enough to justify, if a CS student studying security can only learn by breaking in, special labs and testbeds should be used (controlled experiments)

hackers defense

4) “keeping Big Brother at bay.”

most computer users are unaware but hackers can see systems “inside”

hackers defense

4) “keeping Big Brother at bay.”

most computer users are unaware but hackers can see systems “inside”

a very strong argument however:

1- is the cost of tolerating hackers is what is gained in protection?

hackers defense

4) “keeping Big Brother at bay.”

most computer users are unaware but hackers can see systems “inside”

a very strong argument however:

1- is the cost of tolerating hackers is what is gained in protection?

2- do hackers solve the problem or make it worse?

why not nation-wide protection? if govns can’t be trusted computer professionals can take a step

hackers defense

4) “keeping Big Brother at bay.”

most computer users are unaware but hackers can see systems “inside”

a very strong argument however:

1- is the cost of tolerating hackers is what is gained in protection?

2- do hackers solve the problem or make it worse?

why not nation-wide protection? if govns can’t be trusted computer professionals can take a step

trading one problem for another isn’t a good idea

hackers defense

4) “keeping Big Brother at bay.”

most computer users are unaware but hackers can see systems “inside”

a very strong argument however:

1- is the cost of tolerating hackers is what is gained in protection?

2- do hackers solve the problem or make it worse?

why not nation-wide protection? if govns can’t be trusted computer professionals can take a step

trading one problem for another isn’t a good idea

enormous potential of Internet makes us listen to counter currents even when we don’t agree with them

penalties for hacking

in US, maximum penalties for hacking are severe by Abuse Act:

- transmitting code that causes damage to a computer system
- unauthorized access (even if nothing done!)
- transmitting classified govn info
- trafficking in computer passwords
- computer fraud

penalties for hacking

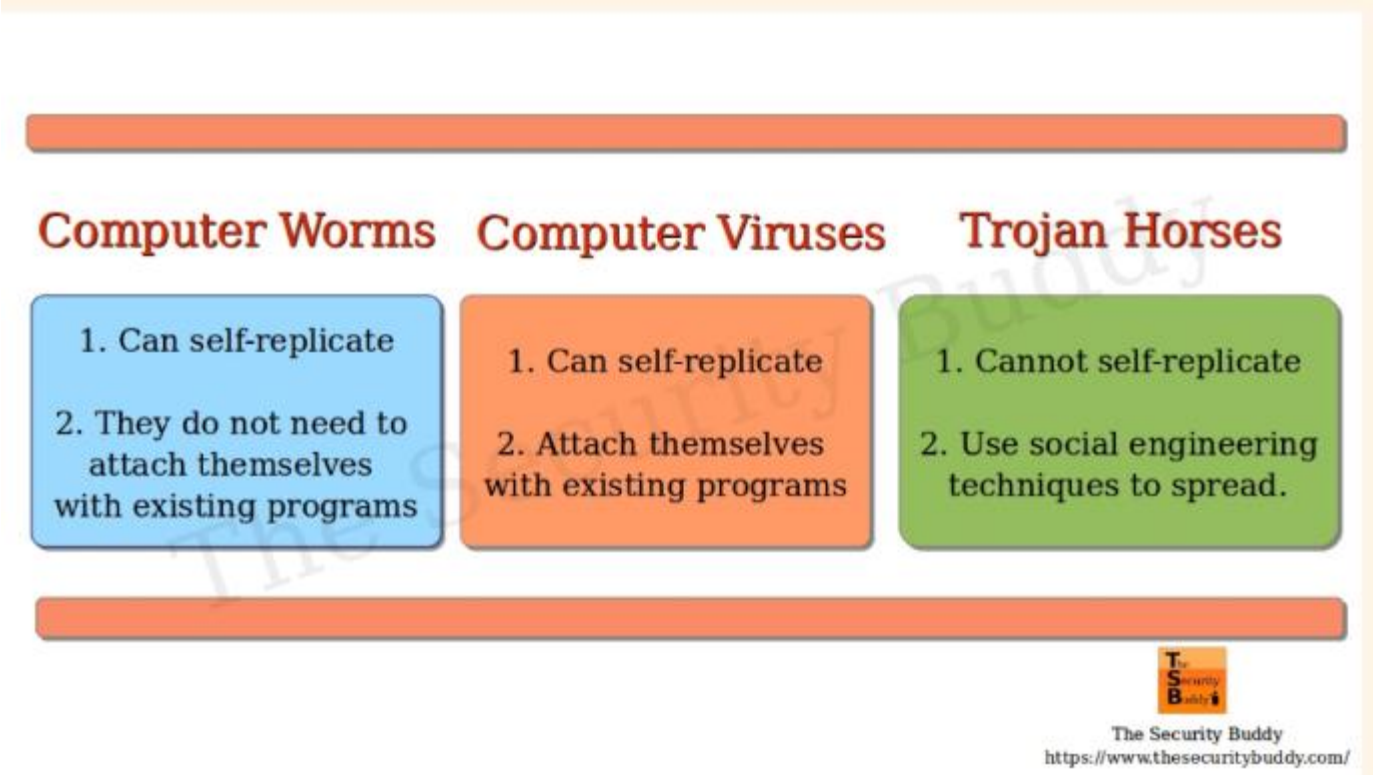
in US, maximum penalties for hacking are severe by Abuse Act:

- transmitting code that causes damage to a computer system
- unauthorized access (even if nothing done!)
- transmitting classified govn info
- trafficking in computer passwords
- computer fraud **(max: 20 yrs prison + $250.000)**

viruses, worms and trojan horses

lucky -> CPU time, disk space

not lucky -> destroyed data, losing control of computer

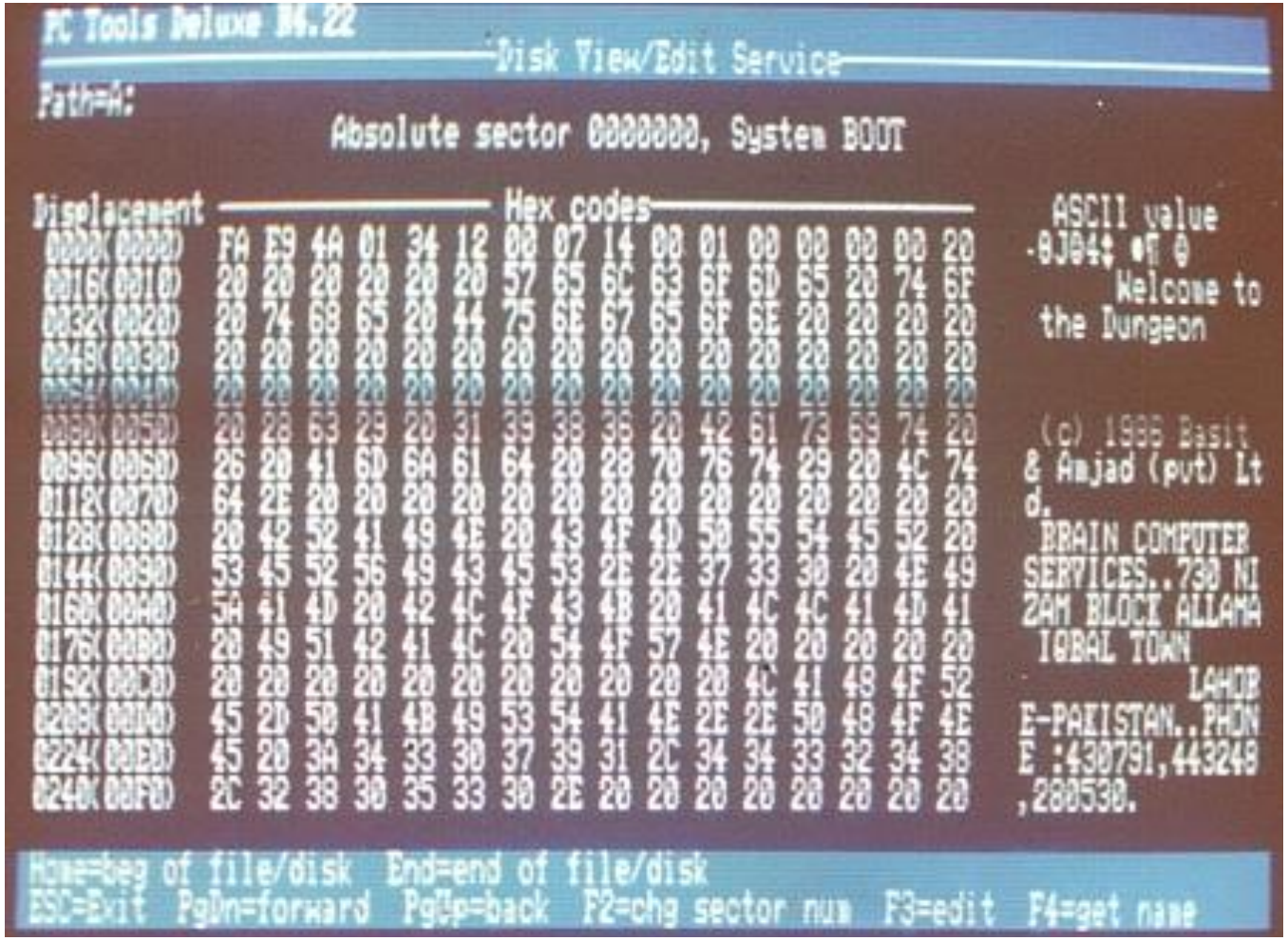


viruses

self-replicating code embedded within another program called the “host”

viruses

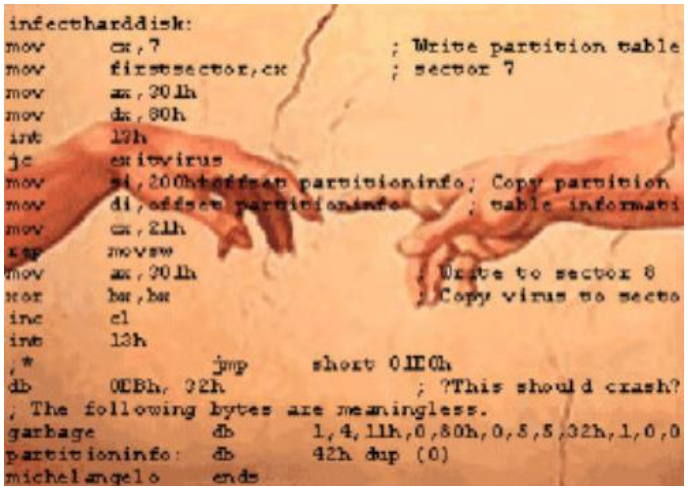
1986 , **Brain** (Pakistani)



viruses

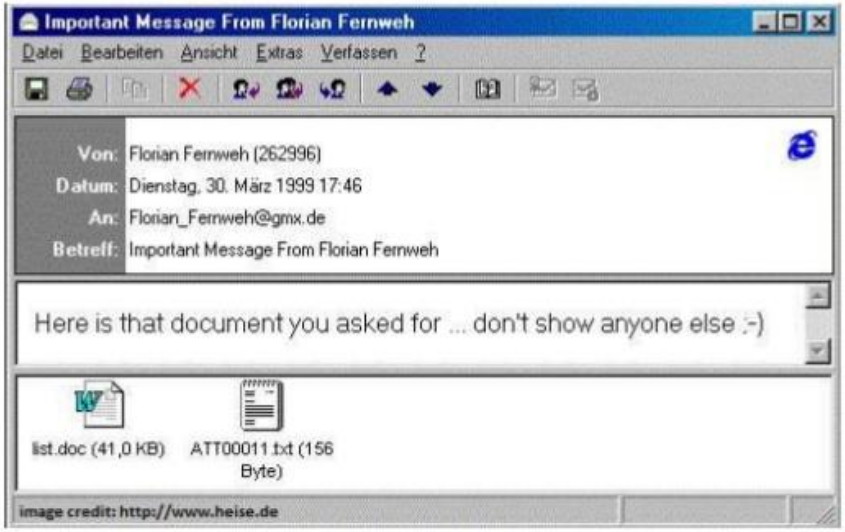
1986 , **Brain** (Pakistani)

1991, **Michelangelo**, if an infected file run on March 6th (birthday) it overwrites critical records on boot disk, media reports over 5 million PCs infected, a through investigation revealed only a few thousand computers in fact



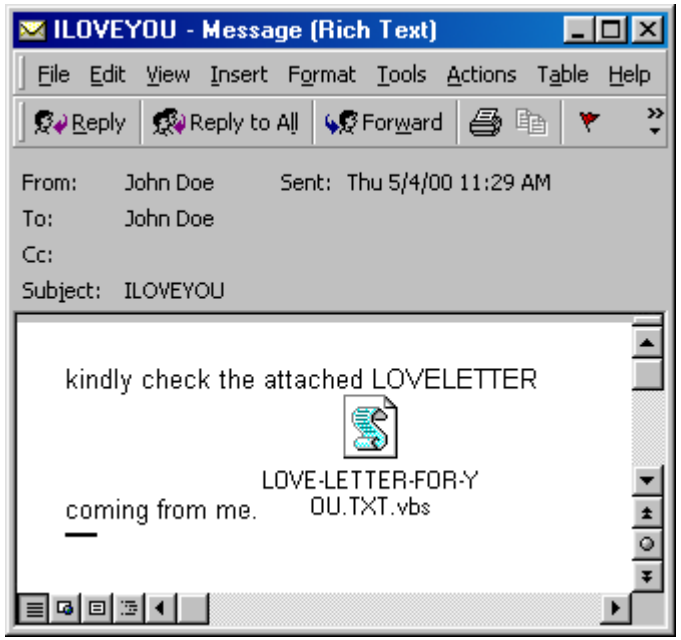
viruses

1999, **Melissa**, email attachment in a word doc, to 50 ppl from victims address book, crashing email servers, 100.000 computers infected at first weekend, David L. Smith, alt.sex.usenet group post, 20 months in prison + 100 hrs community service + $5000



viruses

2000, **Love Bug**, everyone in victim's address book, collects pws and emails in Philipinnes, 23 yrs old Filipino CS student, no laws against hacking in Philipinnes -> no trial held



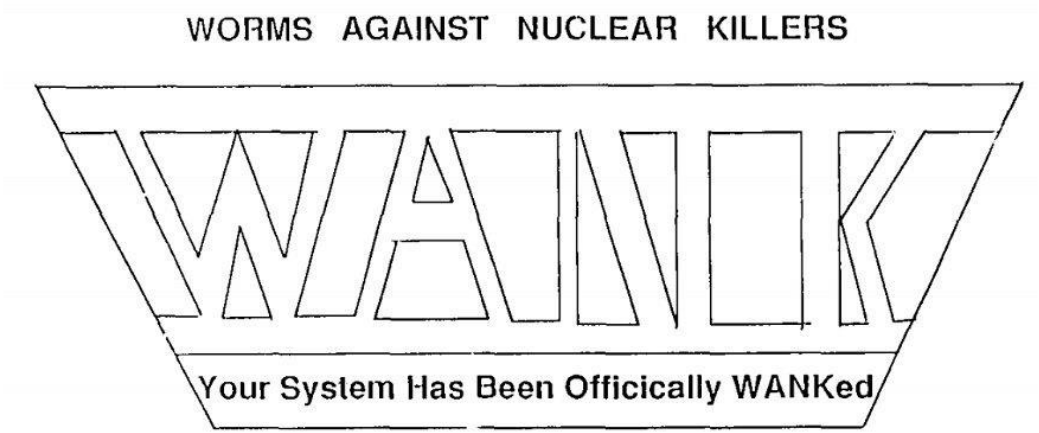
worms

self-contained program spreading through networked computers using security holes

worms

1989, **Wank**, NASA probe to Jupiter named Galileo, fueled with radioactive plutonium, infiltrated NASA network,

anti-nuclear protesters, a case of cyberterrorism, no delay on launch but took a lot of sys admin time to eradicate



worms

2001, **Code Red**, MS IIS bug, Windows web servers

based on the day of month, 1- propagate to others, 2- DoS attacks against whitehouse, 3- sleep, infected more than 359000 hosts in 14 hours

worms

2003, **Sapphire a.k.a. Slammer**, fastest spreading worm in history, doubles in network in every 8,5 seconds, within 10 minutes %90 of vulnerable hosts get infected, at least 78000 computers worldwide, MS SQL Server and MS SQL Desktop Engine bug, not malicious but overloading networks, inaccessible databases (cancelled airline flights, unavailable ATMs, failures in emergency call services)

Spread of Sapphire Worm

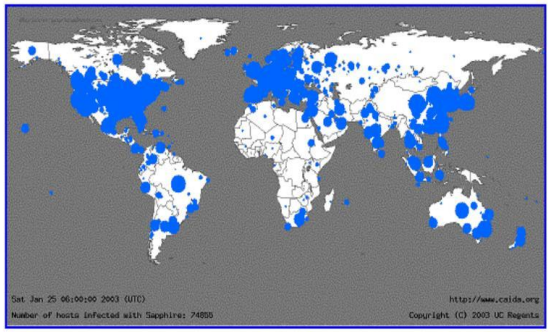
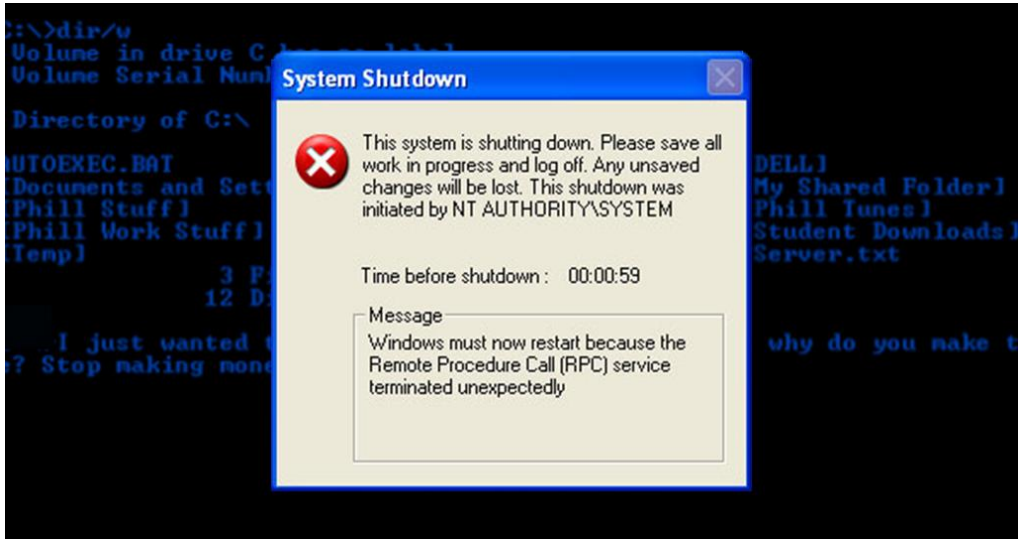


Figure: The geographic spread of Sapphire in the 30 minutes after release.

Source: http://www.cs.berkeley.edu/~nweaver/sapphire/

worms

2003, **Blaster**, bug on Windows 2000 and Windows XP computers, DoS attack against windowsupdate.com, prevents users to download the patch, it actually targets a shortcut to site address, MS deleted the shortcutted address, slowing down systems (disrupted signaling of various train systems)



worms

2004, **Sasser**, already known security weakness in Windows computers, 18 million computers infected without the patch, benign but forces shutdown after reboot (disrupted ops at Delta Airlines, European Commission, Australian railroad system, British coast guard system

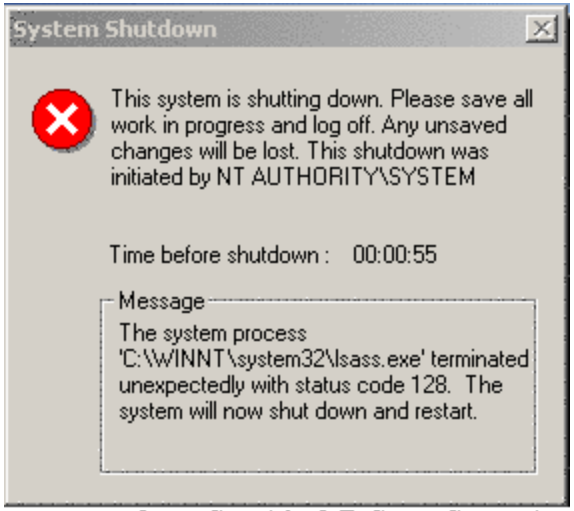


Image Copyright © F-Secure Corporation

worms

2004, **Sasser**, already known security weakness in Windows computers, 18 million computers infected without the patch, benign but forces shutdown after reboot (disrupted ops at Delta Airlines, European Commission, Australian railroad system, British coast guard system

MS put $250.000 reward for headhunt, a fellow student targets a German teen – Sven Jaschan, 17 yrs old when worm released, juvenile court, 1,5 yrs probation + 30 hrs of community service, hired by German computer security firm SecurePoint

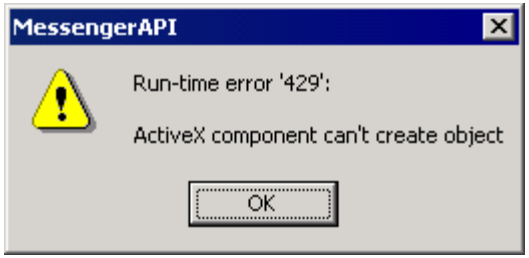
worms

instant messaging worms, 2001, Choke and Hello, not much problems because onl 141 million ppl had been using instant msging in 2001

worms

instant messaging worms, 2001, Choke and Hello, not much problems because onl 141 million ppl had been using instant msging in 2001

2005, **Kelvir**, Reuters News remove 60000 subscribers from its MS-based instant msg services for 20 hrs



worms

the Internet worm...

e.g. 1988, Robert Tappan Morris, Jr., Cornell CS grad student launched a computer worm, most sophisticated of its time, when a site gets infected it would signal to a popular computer system at Berkeley called “Ernie”

worms

Unix OS systems at high school, his father was computer security researcher at Bell Labs, Morris focused on security holes in Unix systems, undergrad student at Harvard CS, quickly become lab's Unix expert, after freshmen year worked at Bell Labs, technical report on security hole of a Berkeley Unix system

worms

Unix OS systems at high school, his father was computer security researcher at Bell Labs, Morris focused on security holes in Unix systems, undergrad student at Harvard CS, quickly become lab's Unix expert, after freshmen year worked at Bell Labs, technical report on security hole of a Berkeley Unix system

Morris, enrolled Cornell CS grad at fall 1988, exploting bugs he found in 3 Unix apps, *ftp*, *sendmail* and *fingerd*

worms

buffer overflow attack to take control of a target computer... based on function calls, **variable attack** -> targets a variable by buffer overflow, **stack attack** -> changing the value of the return address of function call

wishlist of worm had 24 goals including:

- infect three machines per LAN
- only consume CPU cycles if machines are idle
- avoid slow machines
- break pws to spread into other computers

worms

November 2, 1988, ftp bug fix had been posted to Internet, ftp infection down, however sendmail and fingerd apps still vulnerable, logged to MIT AI lab and launched the worm at 07:30

worms

November 2, 1988, ftp bug fix had been posted to Internet, ftp infection down, however sendmail and fingerd apps still vulnerable, logged to MIT AI lab and launched the worm at 07:30

immediately thousand of computers at military, medical and university facilities are infected

worms

November 2, 1988, ftp bug fix had been posted to Internet, ftp infection down, however sendmail and fingerd apps still vulnerable, logged to MIT AI lab and launched the worm at 07:30

immediately thousand of computers at military, medical and university facilities are infected

unfortunately computers become infected with hundreds of copies of the same worm causing crash every few minutes

worms

within 48 hrs the worm is isolated, decompiled and destroy notices are spread, worm did no perm damage but slowed systems to standstill and acquired pws. Morris kicked by university board, trial in 1990, Morris revealed that he tried to stop the worm realizing his mistake, contacted friend from Harvard, Andrew Sudduth confirmed request but solution couldn’t reach because of clogged networks, about 6000 unix computers were infected with the worm

worms

Andrew Sudduth's message:

a possible virus report:

there may be a virus loose on the internet, here is the gist of message I got: **I'm sorry**

here are some steps to prevent further transmission:

1) don't run finger or fix it to not overrun of its stack when reading arguments

2) recompile sendmail w/o DEBUG defined

3) don't run rexed

hope this helps, but more, **I hope it is hoax.**

worms

Harvard’s computers not affected because they had already patched the security holes, Sudduth’s can still not believe Morris’ story, his mail was supposed to routed over computers at Brown university but Brown university computers were already down, the msg subject was also blank anyway, msg read too late...

worms

Harvard's computers not affected because they had already patched the security holes, Sudduth's can still not believe Morris' story, his mail was supposed to routed over computers at Brown university but Brown university computers were already down, the msg subject was also blank anyway, msg read too late...

Morris fould guilty, 3 yrs probation + $10000 fine + 400 hrs of community service... it could easily be 5 yrs jail + $250000 fine if no good defense, his legal fees and fines exceeded $150000

worms

Morris defense: expose a flaw in system because system admins didn't listen to him, he didn't mean such damage but worm got out of control

this is actually similar to a "whistle-blowing" incident

trojan horses

a program with benign capability that conceals another, sinister purpose

trojan horses

a program with benign capability that conceals another, sinister purpose

- opening an Internet connection for an outsider to gain access

trojan horses

a program with benign capability that conceals another, sinister purpose

- opening an Internet connection for an outsider to gain access
- logging keystrokes, searching pws and reporting

trojan horses

a program with benign capability that conceals another, sinister purpose

- opening an Internet connection for an outsider to gain access
- logging keystrokes (keylogger), searching pws and reporting
- destroying files, launching DoS attacks from victim

trojan horses

a program with benign capability that conceals another, sinister purpose

- opening an Internet connection for an outsider to gain access
- logging keystrokes (keylogger), searching pws and reporting
- destroying files, launching DoS attacks from victim
- turning victim computer into a proxy (bot) to launch spam and commit illegal activities

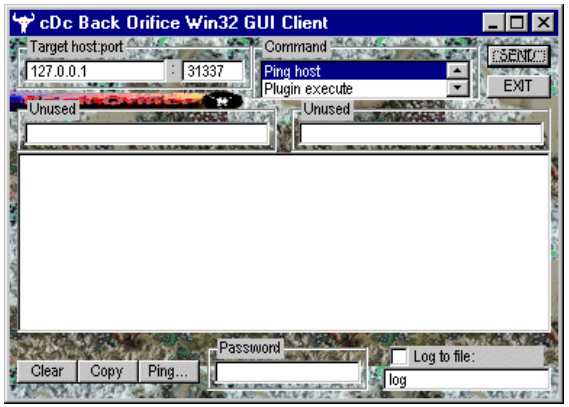
trojan horses

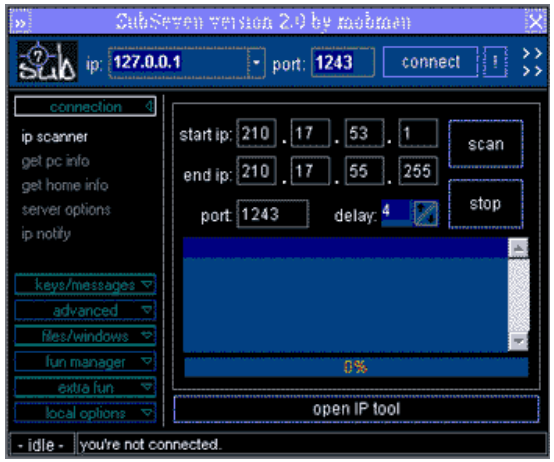
remote access trojan (RAT) -> access to victim computer

trojan horses

remote access trojan (RAT) -> access to victim computer

Back Orifice and **SubSeven** popular. **<u>SubSeven</u>** is notable because of its easy to use point and click user interface, client prg on attacker, server prg on victim, able to capture screenshots, record keystrokes, rd and wr files, watch traffic





trojan horses

remote access trojan (RAT) -> access to victim computer

Back Orifice and **SubSeven** popular. **SubSeven** is notable because of its easy to use point and click user interface, client prg on attacker, server prg on victim, able to capture screenshots, record keystrokes, rd and wr files, watch traffic, **even control the mouse**

trojan horses

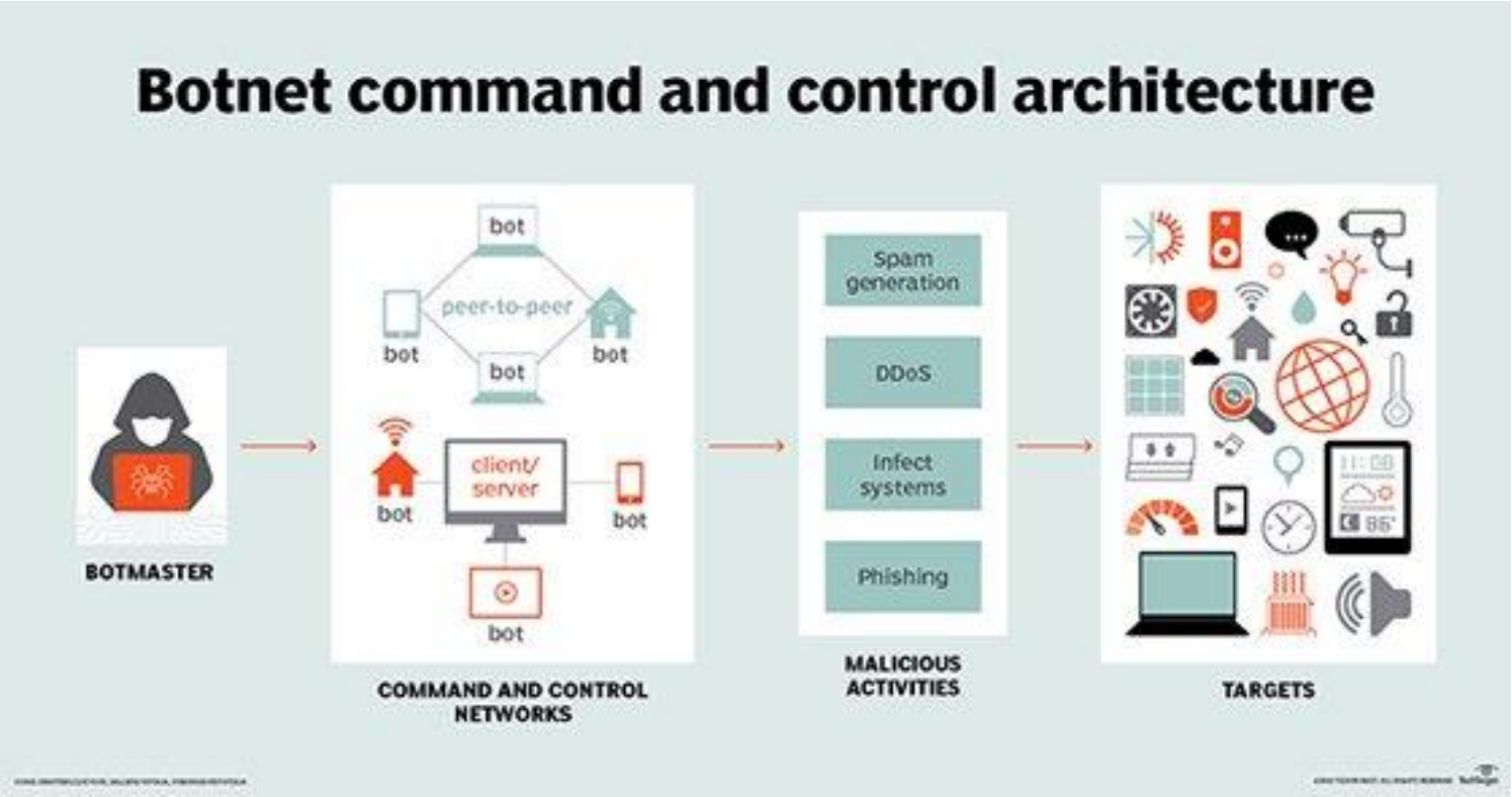
remote access trojan (RAT) -> access to victim computer

Back Orifice and **SubSeven** popular. **SubSeven** is notable because of its easy to use point and click user interface, client prg on attacker, server prg on victim, able to capture screenshots, record keystrokes, rd and wr files, watch traffic, **even control the mouse**

most popular way, distribute as erotica

bot networks

a software program that respons to commands sent by a command-and-control program located on an external computer



bot networks

a software program that respons to commands sent by a command-and-control program located on an external computer

bot-supported legitimate apps: Internet relay chat channels, multiplay Internet games

bot networks

a software program that respons to commands sent by a command-and-control program located on an external computer

bot-supported legitimate apps: Internet relay chat channels, multiplayer Internet games

over %90 of spam is distributed through bot networks, some other bots are designed to steal personal data linked to identity info, bot also can be used for distributed DoS attacks

DoS attacks

intentional action design to prevent legitimate users from making use of a computer service

no stealing here, instead disrupting a computer server’s ability to respond its clients

DoS attacks

intentional action design to prevent legitimate users from making use of a computer service

no stealing here, instead disrupting a computer server's ability to respond its clients

it is an example of "asymmetric" attack, linked with terrorist organizations and much fears about future over this issue

DoS attacks

2000, 15 y.o. boy, DoS attacks disabling many websites including Amazon, eBay, Yahoo, CNN, Dell... “Mafiaboy” was sentenced to 8 months in a juvenile detention center + 1 yr probation

DoS attacks

2000, 15 y.o. boy, DoS attacks disabling many websites including Amazon, eBay, Yahoo, CNN, Dell... “Mafiaboy” was sentenced to 8 months in a juvenile detention center + 1 yr probation

2002, DoS attack to Internet’s 13 root servers that matches IP address to domain names

DoS attacks

2000, 15 y.o. boy, DoS attacks disabling many websites including Amazon, eBay, Yahoo, CNN, Dell... “Mafiaboy” was sentenced to 8 months in a juvenile detention center + 1 yr probation

2002, DoS attack to Internet’s 13 root servers that matches IP address to domain names

recent DoS attacks target blacklisters, CEO of Spamhaus: “we’re usually under attack from 5000 to 10000 servers at once”

DoS attacks

most primitive -> cut off network connection, yet very effective, secure physically first ☺

DoS attacks

most primitive -> cut off network connection, yet very effective, secure physically first ☺

flooding attack, attacker SYN msg by IP-spoofing (like coming from another), target SYN-ACK msg, TCP comm. link standby, as many as SYN msgs, server is in trouble at giving service to legitimate clients

DoS attacks

most primitive -> cut off network connection, yet very effective, secure physically first ☺

flooding attack, attacker SYN msg by IP-spoofing (like coming from another), target SYN-ACK msg, TCP comm. link standby, as many as SYN msgs, server is in trouble at giving service to legitimate clients

smurf attack, first identify broadcasting routers in victims network, ping-echo scheme, spoof again on target for this time, echos to target, target’s nw gets saturated

DoS attacks

filling available space on harddisk of victim:

- email bombing
- worms that generate very long streams of errors, computer logs errors and disk is full
- break in victim and make copies of copies

DoS attacks

filling available space on harddisk of victim:

- email bombing
- worms that generate very long streams of errors, computer logs errors and disk is full
- break in victim and make copies of copies

crashing victim by sending unexpected data, such as an oversized IP packet

DoS attacks

filling available space on harddisk of victim:

- email bombing
- worms that generate very long streams of errors, computer logs errors and disk is full
- break in victim and make copies of copies

crashing victim by sending unexpected data, such as an oversized IP packet

distributed DoS attacks, botherder and many bots, DDoS is a kind of smurf attack from thousands of computers (instead of only one)

DoS attacks

Blue Security, Israeli company, spam-deterrence system, fighting bots with bots, sold service to businesses, free for end-users, users download a bot called "Blue Frog", integrated with Yahoo, Gmail and Hotmail, checking email msgs for spam, when a spam is found bot contacts to Blue Security server to determine the source of email, **<u>then the bot would send the spammer an opt-out msg</u>**

BLUE SECURITY
SMARTER, SAFER

DoS attacks

spammers targeting millions of addresses started receiving thousands of automatically generated opt-out msgs filling their networks and disrupting their ops

DoS attacks

spammers targeting millions of addresses started receiving thousands of automatically generated opt-out msgs filling their networks and disrupting their ops

6 of the world's top 10 spammers agreed to use Blue Security's filtering sw to remove Blue Frog users from their email lists

DoS attacks

One spammer, PharmaMaster didn't back down, he even threatened Blue Frog users: **"Unfortunately, due to tactics used by Blue Security, you will end up receiving this message and other nonsensical spams 20-40 times than you would normally."**

DoS attacks

One spammer, PharmaMaster didn't back down, he even threatened Blue Frog users: **"Unfortunately, due to tactics used by Blue Security, you will end up receiving this message and other nonsensical spams 20-40 times than you would normally."**

followed threats and may 1, 2006 sending Blue Frog users 10 to 20 times more spam as they would normally receive

DoS attacks

the next day PharmaMaster directed Blue Security itself, massive DDoS attack from ten thousands of bots targeting Blue Security's servers

DoS attacks

the next day PharmaMaster directed Blue Security itself, massive DDoS attack from ten thousands of bots targeting Blue Security's servers

first Blue Frog services went down... then he targeted other companies providing Internet services to Blue Security... then he targeted the businesses that pay for Blue Security services

DoS attacks

the next day PharmaMaster directed Blue Security itself, massive DDoS attack from ten thousands of bots targeting Blue Security's servers

first Blue Frog services went down... then he targeted other companies providing Internet services to Blue Security... then he targeted the businesses that pay for Blue Security services... **all down...**

DoS attacks

when Blue Security realized it could not protect **<u>its business customers</u>** from DDoS attacks and virus-laced emails, it reluctantly discontinued its service:

{* THE CHANNEL *}

Blue Security calls it quits after attack by renegade spammer

Folds spam fighting operation

Wed 17 May 2006 // 14:07 UTC

GOT TIPS?

Google C

DoS attacks

when Blue Security realized it could not protect **<u>its business customers</u>** from DDoS attacks and virus-laced emails, it reluctantly discontinued its service:

Eran Rashef, CEO of Blue Security announced: **"We cannot take the responsibility for an everescalating cyberwar through our continued operations. We are discontinuing all of our anti-spam activities."**

DoS attacks

when Blue Security realized it could not protect **<u>its business customers</u>** from DDoS attacks and virus-laced emails, it reluctantly discontinued its service:

Eran Rashef, CEO of Blue Security announced: **"We cannot take the responsibility for an everescalating cyberwar through our continued operations. We are discontinuing all of our anti-spam activities."**

Blue Security's decision to fight bots with bots – always controversial – **<u>was ultimately unsuccessful</u>**

DoS attacks

1995, computer security expert, Dan Farmer, Security Administrator Tool for Analyzing Networks (SATAN), probing security weaknesses automatically

SATAN

(Security Administrator Tool for Analyzing Networks)

DoS attacks

1995, computer security expert, Dan Farmer, Security Administrator Tool for Analyzing Networks (SATAN), probing security weaknesses automatically

easy to use interface tempted teenagers into computer hackers, easy to create scripts for hackers to probe hundreds of sites and report their security holes, Farmer admitted that SATAN is **"a two-edged sword that can be used for good and evil"**

DoS attacks

1995, computer security expert, Dan Farmer, Security Administrator Tool for Analyzing Networks (SATAN), probing security weaknesses automatically

easy to use interface tempted teenagers into computer hackers, easy to create scripts for hackers to probe hundreds of sites and report their security holes, Farmer admitted that SATAN is **"a two-edged sword that can be used for good and evil"**

as it turns out, SATAN-enabled computer break-ins never materialized

DoS attacks

+2 yrs after release, Dan Farmer survey the security of 2200+ websites, %60 sites vulnerable to break-ins, about half of them had major security problems even though all of the security holes probed by SATAN had been publicized

defensive measures

skill and dedication of sys admins + cooperation of nw users

defensive measures

skill and dedication of sys admins + cooperation of nw users

authorization (permissions), authentication (knowledge based – pw, tokes – ID card, smart card, biometrics – fingerprint, retinal scan) highly secure systems are more likely to go multilevel

defensive measures

skill and dedication of sys admins + cooperation of nw users

authorization (permissions), authentication (knowledge based – pw, tokes – ID card, smart card, biometrics – fingerprint, retinal scan) highly secure systems are more likely to go multilevel

most common pw, prevent easy guess (circulars), foil dictionary attack (add a non alpha char)

defensive measures

skill and dedication of sys admins + cooperation of nw users

authorization (permissions), authentication (knowledge based – pw, tokes – ID card, smart card, biometrics – fingerprint, retinal scan) highly secure systems are more likely to go multilevel

most common pw, prevent easy guess (circulars), foil dictionary attack (add a non alpha char)

installing firewalls between “inside” and “outside”, virus filters

defensive measures

skill and dedication of sys admins + cooperation of nw users

authorization (permissions), authentication (knowledge based – pw, tokes – ID card, smart card, biometrics – fingerprint, retinal scan) highly secure systems are more likely to go multilevel

most common pw, prevent easy guess (circulars), foil dictionary attack (add a non alpha char)

installing firewalls between “inside” and “outside”, virus filters, **up-to-date systems**

Internet Banking: Client-Side Attacks and Protection Mechanisms

by Rolf Oppliger, Ruedi Rytz and Thomas Holderegger, 2009

some banks pw and PINs, others use transaction authentication and authorization numbers (TANs)

many researchers have analyzed the SSL(Secure Sockets Layer)/TLS(Transport Layer Security) protocol's security, but have identified only a few theoretical shortcomings and vulnerabilities

Internet Banking

communication channel security focus... but

Internet Banking

communication channel security focus... but

in fact, an adversary has many ways to attack the client, **the client represents the major vulnerability**, installing many kinds of plug-ins on their client systems

Internet Banking

communication channel security focus... but

in fact, an adversary has many ways to attack the client, **the client represents the major vulnerability**, installing many kinds of plug-ins on their client systems

just a good cover story... use social engineering techniques

client side attacks

1) credential stealing attack

either directly (poor defense), or indirectly (tricking) -> phishing, pharming, visual spoofing

attacker gathers data, uses later to spoof identity, **offline attacks**

client side attacks

2) channel-breaking attack

attacker cryptanalyze SSL/TLS protocol, studied in theory, none has been particulary successful in practice

instead Man-in-the-Middle (MITM) attack, mounted in real-time, **online attacks**

client side attacks

3) content-manipulation attack

man-in-the-browser attack, browser poisoning, alarming potential, only solution is the removal of malware which is difficult and even impossible forcing a reinstallation of system

client side attacks

3) content-manipulation attack

man-in-the-browser attack, browser poisoning, alarming potential, only solution is the removal of malware which is difficult and even impossible forcing a reinstallation of system

a browser can display correct data but still transmit manipulated data to server

protection against offline credential-stealing attacks

two-factor authentication, combining a hardware token with a PIN to unlock it (SecureID, Secure One Time Verification - SecOVID, challenge-response system)

two-factor authentication – <u>if properly designed and implemented</u> – can effectively protect against most offline credential stealing attacks

protection against online channel-breaking attacks

1) the banking server application can try to enforce a proper server certificate validation (and hence ensure that the user is connected to the proper server) (extended validation SSL – EV-SSL)

protection against online channel-breaking attacks

1) the banking server application can try to enforce a proper server certificate validation (and hence ensure that the user is connected to the proper server) (extended validation SSL – EV-SSL)

2) the banking server application can invoke mechanisms that are specifically crafted to protect against MITM attacks

protection against online channel-breaking attacks

1) the banking server application can try to enforce a proper server certificate validation (and hence ensure that the user is connected to the proper server) (extended validation SSL – EV-SSL)

2) the banking server application can invoke mechanisms that are specifically crafted to protect against MITM attacks **(also suggested using multiple communication channels, requiring SMS codes etc.)**

protection against content-manipulation attacks

1) bank or user can try to protect the Internet banking client from manipulation

2) the bank can have the client to authenticate the transactions (in addition to user authentication)

protection against content-manipulation attacks

1) bank or user can try to protect the Internet banking client from manipulation

2) the bank can have the client to authenticate the transactions (in addition to user authentication)

they aren’t mutually exclusive, both can be used at the same time

client protection

1) dedicated client system (quite expensive approach)

client protection

1) dedicated client system (quite expensive approach)

2) dedicated client software (technically feasible but the bank must act as a software distributor)

client protection

1) dedicated client system (quite expensive approach)

2) dedicated client software (technically feasible but the bank must act as a software distributor)

3) live distribution (bootable OSs supported by bank, usability problem)

client protection

1) dedicated client system (quite expensive approach)

2) dedicated client software (technically feasible but the bank must act as a software distributor)

3) live distribution (bootable OSs supported by bank, usability problem)

4) virtual machine (e.g. VMWare or QEMU, solution's security remains a research challenge)

client protection

1) dedicated client system (quite expensive approach)

2) dedicated client software (technically feasible but the bank must act as a software distributor)

3) live distribution (bootable OSs supported by bank, usability problem)

4) virtual machine (e.g. VMWare or QEMU, solution's security remains a research challenge)

5) browser operating system (ongoing research projects)

Internet OS

From Wikipedia, the free encyclopedia

client protection

1) dedicated client system (quite expensive approach)

2) dedicated client software (technically feasible but the bank must act as a software distributor)

3) live distribution (bootable OSs supported by bank, usability problem)

4) virtual machine (e.g. VMWare or QEMU, solution's security remains a research challenge)

5) browser operating system (ongoing research projects)

6) trusted computing (special hw device that ensures the system boot into a secure state, resarch area, still can be exploited)

transaction authentication

following a user request, SMS message including: summary of transaction + confirmation code

researchers expect many Internet banks to begin using transaction authentication with specific heuristics in future

sociotechnical security

reliability in IT systems is broader than security ->>> security + well-design

security is an instrumental value to IT systems

sociotechnical security

reliability in IT systems is broader than security ->>> security + well-design

security is an instrumental value to IT systems

security is achieved sociotechnically

sociotechnical security

reliability in IT systems is broader than security ->>> security + well-design

security is an instrumental value to IT systems

security is achieved sociotechnically

“strong password”+forcing but how about carelessness?

a single careless user compromises the security of whole system (30 computer business, hw+sw auth, superb passes, biometric scans, fingerprints, monitoring traffic, card system entry... no 100% security)

sociotechnical security

threat comes especially from inside:

- open backdoor for pizza delivery

sociotechnical security

threat comes especially from inside:

- open backdoor for pizza delivery
- lending pw to daugther on “take your daughter to work” day :p

sociotechnical security

threat comes especially from inside:

- open backdoor for pizza delivery
- lending pw to daugther on “take your daughter to work” day :p
- admin using wife’s firstname for root pw

sociotechnical security

threat comes especially from inside:

- open backdoor for pizza delivery
- lending pw to daugther on “take your daughter to work” day :p
- admin using wife’s firstname for root pw

security has to be implemented sociotechnically to achieve its goal! any missteps in either arena... then the system is vulnerable

sociotechnical security

STS coshaping scheme here again:

intruder must also be adept at “social engineering” -> fooling people

sociotechnical security

STS coshaping scheme here again:

intruder must also be adept at “social engineering” -> fooling people

... bottomline: “security arms race”

sociotechnical security

STS coshaping scheme here again:

intruder must also be adept at “social engineering” -> fooling people

... bottomline: “security arms race”

no need to discuss more on intruder... how about who’s responsible for security breaches and security tradeoffs?

also be careful on “dumpster diving”

who is to blame in security breaches?

intruder obviously faulty, but who’s responsible for security?

who is to blame in security breaches?

intruder obviously faulty, but who's responsible for security?

security of PC ~ usually individual computer owner

installation of security mechanisms -> burden + cost

who is to blame in security breaches?

intruder obviously faulty, but who's responsible for security?

security of PC ~ usually individual computer owner

installation of security mechanisms -> burden + cost

if one doesn't take a security step can they be – partially at least – blamed when an intruder breaks in?

who is to blame in security breaches?

home analogy -> from changing region to sophisticated household systems

who is to blame in security breaches?

home analogy -> from changing region to sophisticated household systems

but need for money -> if able and didn’t do -> foolish!!!

who is to blame in security breaches?

home analogy -> from changing region to sophisticated household systems

but need for money -> if able and didn't do -> foolish!!!

BUT! still not contributed to wrongdoing.

who is to blame in security breaches?

home analogy -> from changing region to sophisticated household systems

but need for money -> if able and didn't do -> foolish!!!

BUT! still not contributed to wrongdoing.

however IT-configured societies -> complicated issue again

if A is a part of larger system B, any risk at A puts B at risk. "drone attacks"

trade-offs in security

how far should security and law enforcements go to ensure order?

previous issue: micro-level / individual level

current issue: macro-level / what should we do as a society? how should we allow our govns do things wrt security?

trade-offs in security

how far should security and law enforcements go to ensure order?

previous issue: micro-level / individual level

current issue: macro-level / what should we do as a society? how should we allow our govns do things wrt security?

11.09.2001... US patriot act with ease... in 2007, FBI abuse, 3 yrs period 143000 national security letters for customer purchases

trade-offs in security

how far should security and law enforcements go to ensure order?

previous issue: micro-level / individual level

current issue: macro-level / what should we do as a society? how should we allow our govns do things wrt security?

11.09.2001... US patriot act with ease... in 2007, FBI abuse, 3 yrs period 143000 national security letters for customer purchases, **non-terrorist related acts can now be investigated legally** (security X privacy conflict)

wikipedia: a new order of knowledge production

reliability is also valuable for knowledge production

684 million use Wikipedia each year

wikipedia: a new order of knowledge production

reliability is also valuable for knowledge production

684 million use Wikipedia each year

consensus vs. credential issue

wikipedia: a new order of knowledge production

reliability is also valuable for knowledge production

684 million use Wikipedia each year

consensus vs. credential issue

alternative reliability approach

“proof is in the pudding” -> to fully test something you need to experience it yourself

wikipedia: a new order of knowledge production

reliability is also valuable for knowledge production

684 million use Wikipedia each year

consensus vs. credential issue

alternative reliability approach

“proof is in the pudding” -> to fully test something you need to experience it yourself

“the many” vs. “the few”

“voice of the crowd” -> democracy?

freedom of expression and censorship

emblematic of democracy... no high degree of freedom of expression → no democracy

freedom of expression and censorship

emblematic of democracy... no high degree of freedom of expression → no democracy

supported by formal specifications and laws, already complicated matter, Internet made it more complicated

freedom of expression and censorship

John Stuart Mill's 4 arguments (~150 yrs old) still hold for this issue:

1) silencing the voice of truth

freedom of expression and censorship

John Stuart Mill's 4 arguments (~150 yrs old) still hold for this issue:

1) silencing the voice of truth

2) silencing a degree of truth (nothing can be completely true or erroneous)

freedom of expression and censorship

John Stuart Mill's 4 arguments (~150 yrs old) still hold for this issue:

1) silencing the voice of truth

2) silencing a degree of truth (nothing can be completely true or erroneous)

3) whole truth is can be only tested with clash of ideas

freedom of expression and censorship

John Stuart Mill's 4 arguments (~150 yrs old) still hold for this issue:

1) silencing the voice of truth

2) silencing a degree of truth (nothing can be completely true or erroneous)

3) whole truth is can be only tested with clash of ideas

4) an opinion tested in free and open discourse is more likely to have a "vital effect on the character and conduct"

freedom of expression and censorship

now it requires courage to allow free electronic speech on the Internet

restrictions when other important values are at stake;

- harm principle -> (until another is harmed)

freedom of expression and censorship

now it requires courage to allow free electronic speech on the Internet

restrictions when other important values are at stake;

- harm principle -> (until another is harmed)
- offense principle

freedom of expression and censorship

now it requires courage to allow free electronic speech on the Internet

restrictions when other important values are at stake;

- harm principle -> (until another is harmed)
- offense principle -> **(if not careful, can bring an end to free speech)**

freedom of expression and censorship

now it requires courage to allow free electronic speech on the Internet

restrictions when other important values are at stake;

- harm principle -> (until another is harmed)
- offense principle -> **(if not careful, can bring an end to free speech)** (prisoner blogs about murder details

freedom of expression and censorship

now it requires courage to allow free electronic speech on the Internet

restrictions when other important values are at stake;

- harm principle -> (until another is harmed)
- offense principle -> **(if not careful, can bring an end to free speech)** prisoner blogs about murder details, censorship on porno for children --- the "**slippery slope**"

freedom of expression and censorship

now it requires courage to allow free electronic speech on the Internet

restrictions when other important values are at stake;

- harm principle -> (until another is harmed)
- offense principle -> **(if not careful, can bring an end to free speech)** prisoner blogs about murder details, censorship on porno for children --- the "**slippery slope**" ... <u>have already been taken</u>, now the issue is where to draw the line?

freedom of expression and censorship

now it requires courage to allow free electronic speech on the Internet

restrictions when other important values are at stake;

- harm principle -> (until another is harmed)
- offense principle -> **(if not careful, can bring an end to free speech)** prisoner blogs about murder details, censorship on porno for children --- the "**slippery slope**" ... <u>have already been taken</u>, now the issue is where to draw the line?

if govns cave, private orgs will step up, this even can be more dangerous

online voting

2000 presidental election, one of the closest in US history... Florida was pivotal state... Without Florida's electoral votes, neither Bush nor Al Gore could get majority of votes in Electoral College

online voting

2000 presidental election, one of the closest in US history... Florida was pivotal state... Without Florida's electoral votes, neither Bush nor Al Gore could get majority of votes in Electoral College, **4 heavily democratic counties recounted in Florida**:

online voting

2000 presidental election, one of the closest in US history... Florida was pivotal state... Without Florida's electoral votes, neither Bush nor Al Gore could get majority of votes in Electoral College, **4 heavily democratic counties recounted in Florida**:

Florida secretary of state declared that:

Bush: 2,912,790 votes

Gore: 2,912,253 votes

online voting

2000 presidental election, one of the closest in US history... Florida was pivotal state... Without Florida's electoral votes, neither Bush nor Al Gore could get majority of votes in Electoral College, **4 heavily democratic counties recounted in Florida**:

Florida secretary of state declared that:

Bush: 2,912,790 votes

Gore: 2,912,253 votes

what a finish... by 2/10000 difference... **most of these counties used keypunch voting machine**...

online voting

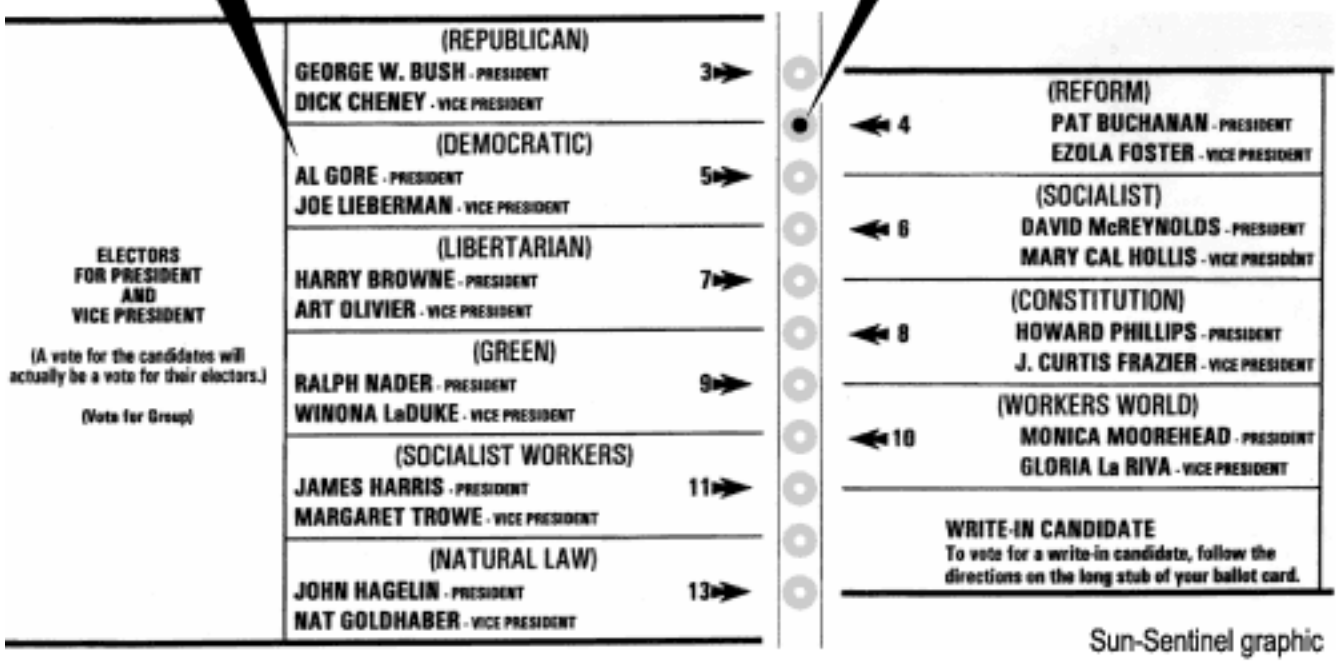
improving reliability of voting systems...

Confusion at Palm Beach County polls

Some Al Gore supporters may have mistakenly voted for Pat Buchanan because of the ballot's design.

Although the Democrats are listed second in the column on the left, they are the third hole on the ballot.

Punching the second hole casts a vote for the Reform party.



Sun-Sentinel graphic

benefits of online voting

who cannot get to polls, ease from home

benefits of online voting

who cannot get to polls, ease from home

counting quickly

benefits of online voting

who cannot get to polls, ease from home

counting quickly

no physical problems (erasures, middle signs)

benefits of online voting

who cannot get to polls, ease from home

counting quickly

no physical problems (erasures, middle signs)

less cost than traditional voting

benefits of online voting

who cannot get to polls, ease from home

counting quickly

no physical problems (erasures, middle signs)

less cost than traditional voting

eliminating the risk of manipulating boxes

benefits of online voting

who cannot get to polls, ease from home

counting quickly

no physical problems (erasures, middle signs)

less cost than traditional voting

eliminating the risk of manipulating boxes

multiple choice (ordered) elections can be easier

benefits of online voting

who cannot get to polls, ease from home

counting quickly

no physical problems (erasures, middle signs)

less cost than traditional voting

eliminating the risk of manipulating boxes

multiple choice (ordered) elections can be easier

complicated and long ballots leading undervoting can be eliminated

risks of online voting

unfair adv. over ppl with computers and Internet connections at home

risks of online voting

unfair adv. over ppl with computers and Internet connections at home

the system authenticates the user, also records the ballot... privacy? ☺

risks of online voting

unfair adv. over ppl with computers and Internet connections at home

the system authenticates the user, also records the ballot... privacy? ☺

vote solicitation and vote selling is easier (watching screen etc.)

risks of online voting

unfair adv. over ppl with computers and Internet connections at home

the system authenticates the user, also records the ballot... privacy? ☺

vote solicitation and vote selling is easier (watching screen etc.)

obvious target for DDoS attacks

risks of online voting

unfair adv. over ppl with computers and Internet connections at home

the system authenticates the user, also records the ballot... privacy? ☺

vote solicitation and vote selling is easier (watching screen etc.)

obvious target for DDoS attacks

vote-tampering viruses

risks of online voting

unfair adv. over ppl with computers and Internet connections at home

the system authenticates the user, also records the ballot... privacy? ☺

vote solicitation and vote selling is easier (watching screen etc.)

obvious target for DDoS attacks

vote-tampering viruses

remote access trojans such as SubSeven

risks of online voting

unfair adv. over ppl with computers and Internet connections at home

the system authenticates the user, also records the ballot... privacy? ☺

vote solicitation and vote selling is easier (watching screen etc.)

obvious target for DDoS attacks

vote-tampering viruses

remote access trojans such as SubSeven

pharming

conclusions on online voting

1) existing systems are highly localized, local corrupts cannot corrupt entire state

conclusions on online voting

1) existing systems are highly localized, local corrupts cannot corrupt entire state

2) paper record and hard copy for backup, when all else fails, you can rely on hard copies, no hard copies in online voting

conclusions on online voting

1) existing systems are highly localized, local corrupts cannot corrupt entire state

2) paper record and hard copy for backup, when all else fails, you can rely on hard copies, no hard copies in online voting

Bruce Scheiner: “A secure Internet voting system is theoretically possible, but it would be the first secure networked application ever created in computing history.”

conclusions on online voting

1) existing systems are highly localized, local corrupts cannot corrupt entire state

2) paper record and hard copy for backup, when all else fails, you can rely on hard copies, no hard copies in online voting

Bruce Scheiner: "A secure Internet voting system is theoretically possible, but it would be the first secure networked application ever created in computing history."

an election system relying on security of personal computers is vulnerable to electoral fraud

conclusions on online voting

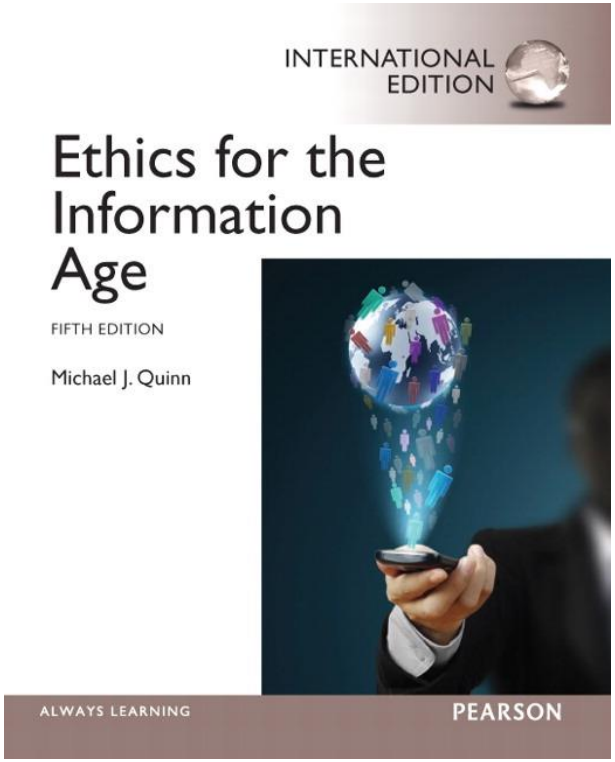
"The anonymity requirements of remote Internet voting generally don't allow the use of transaction authentication and monitoring technologies"
(Oppliger et al., 2009)

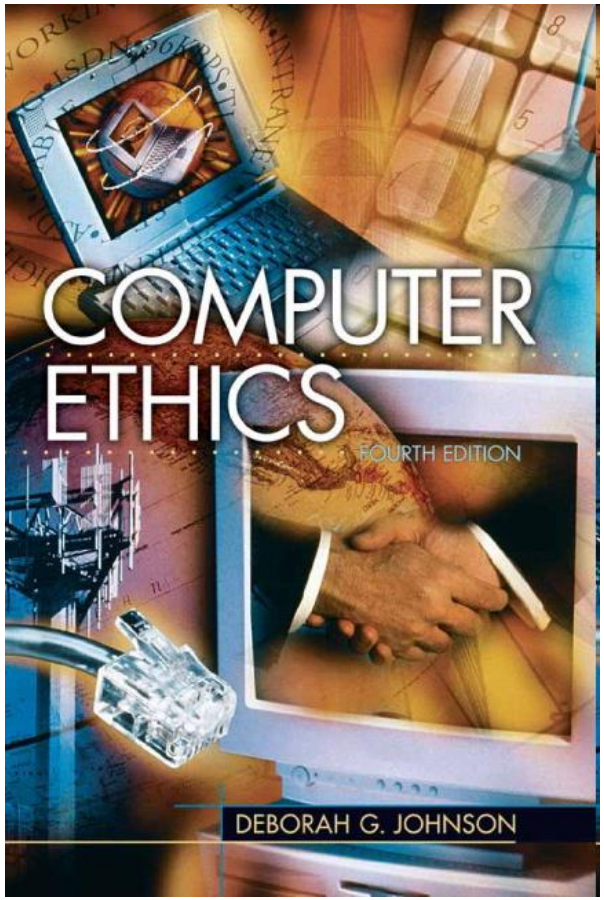
conclusions on online voting

"The anonymity requirements of remote Internet voting generally don't allow the use of transaction authentication and monitoring technologies" (Oppliger et al., 2009)

there is a strong case to be made that a government should <u>not allow</u> online voting to be conducted in this way

references





Google™

WIKIPEDIA