Bad Things in Your In-Box

Richard Clayton

Mike Bond

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

23rd Cambridge International Symposium on Economic Crime

7th September 2005

No time to talk about

- “Your email won the lottery”
- “Your mortgage is approved at 3.5%”
- Advanced Fee Fraud (419 scams)
- Offers of cheque processing jobs
- V!agr@, Pornography, Warez
- I am on vacation
- ¡´ -·¤ô½ü¬yÂà¡A-·¤ô¾Ç¬O¤¤°ê¤-³N¤§¤@¡

What will be covered

- Phishing
- The spam economy
- Viruses & worms
- Open discussion

Why does phishing work?

- Con artists are really, really good at persuading people to do dumb things.
- Almost no context to an email, or a website; so you no longer need an Intaglio-capable printing press to produce plausible props.
- The underlying protocols and procedures are pretty rubbish…

Bank “authentication” protocol

- Alice signs on using her password(s)

  A→B: A, S_n

- Hence there is a Man-In-The-Middle attack

  A→P: A, S_n

  and then later on

  P→B: A, S_n

Sehr geehrter Kunde!

Wir sind erfreut, Ihnen mitzuteilen, dass Internet - Ueberweisungen ueber unsere Bank noch sicherer geworden sind!

Leider wurde von uns in der letzten Zeit, trotz der Anwendung von den TAN-Codes, eine ganze Reihe der Mitteldiebstaehle von den Konten unserer Kunden durch den Internetzugriff festgestellt.

Zur Zeit kennen wir die Methodik nicht, die die Missetaeter fuer die Entwendung der Angaben aus den TAN - Tabellen verwenden. Um die Missetaeter zu ermitteln und die Geldmittel von unseren Kunden unversehrt zu erhalten, haben wir entschieden, aus den TAN - Tabellen von unseren Kunden zwei aufeinanderfolgenden Codes zu entfernen.
Dafuer muessen Sie unsere Seite besuchen, wo Ihnen angeboten wird, eine spezielle Form auszufuellen. In dieser Form werden Sie ZWEI FOLGENDE TAN - CODEs, DIE SIE NOCH NICHT VERWENDET HABEN, EINTASTEN.

Achtung! Verwenden Sie diese zwei Codes in der Zukunft nicht mehr!

Wenn bei der Mittelueberweisung von Ihrem Konto gerade diese TAN - Codes verwendet werden, so wird es fuer uns bedeuten, dass von Ihrem Konto eine nicht genehmigte Transitaktion ablaeuft und Ihr Konto wird unverzueglich bis zur Klaerung der Zahlungsumstaende gesperrt.

Fixing with freshness

- Alice signs on using SecurID, or a one-time password from a booklet, or a token value provided by an SMS message, or some other two-factor time-based authentication token...

  A→B: A, S_n

- MITM **still possible**, albeit only in real time

  A→P: A, S_n

  P→B: A, S_n

Session extension attack

- Alice signs on and does her transactions

  A→B: A, T_1

  A→B: A, T_2

- Phisher extends the session…

  A→P→B: A, T_1

  A→P→B: A, T_2

  P→B: A, T_3

What about `https:` ?

- SSL (or TLS) provides protection against eavesdropping and tampering
- Will also authenticate identity of remote site
- But this is no big win

  P→A: $\{\text{I am site-P}\}_{K^{-1}_{\text{Certifier}}}$

  and unless A concentrates she thinks she has just been told that the other end is “B”

Surely, we can fix it with crypto?

$A \rightarrow B: \quad \{A, B, nonce, Transaction_n\}_{K_A^{-1}}$

Academic community will be delighted to assist in analysing what is within the brackets, ensuring that sufficient information is being signed, checking that you can't use multiple simultaneous protocol runs to mount an attack…

Crypto doesn’t provide trust

- Alice must completely trust the program she is using to do the crypto (because she will not be able to do PKI sums in her head)
- So what if the phisher invites her to download a new improved version from

  `www.bankname.newsoftware.com` ?

  note that *bankname* doesn’t see this being registered! So policing the DNS won’t help

Crypto isn't a complete solution

- We've only really punted – how does the crypto program authenticate Alice?
- How does Alice handle all the "user friendly" indirections?

`PAY GAS COMPANY £100`

is, in actuality, the hard to check

`TRANSFER 100.00GBP to 06-07-08 12346789`

What about browser pop-ups?

- Phishers already overwrite padlocks, the URL being visited and the URL asked for…
  - with current browser "security" models you cannot really rely on *anything* on the screen being in the least bit valid
  - it is not credible to insist consumers check for the browser patches every day **and** also turn off Java, JavaScript, ActiveX and Flash…

    ...besides, the banking site probably needs them!

Is “authentication” the problem?

- Schneier 2005: *If we’re ever going to manage the risks and effects of electronic impersonation, we must concentrate on preventing and detecting fraudulent transactions.*
- His proposes to make financial institutions responsible for all fraudulent transactions...
  - not a solution; but a mechanism to find one

The “spam economy”

- Once upon a time the spam came from the spammers machines
- Now it comes from customer machines that are “0wned” by the spammers
- These 0wned machines are hired out to the highest bidder, initially top end spammers, then run-of-the-mill, then DDoS…

Viruses and worms as tools

- In the good old days, they caused deliberate damage, or were novel experiments, or were just to show off
- Nowadays, they don't *attack* you, they *exploit* you. They log your keystrokes and passwords, or they hijack your machine to send spam
- They are now just **tools** of the trade for gaining and controlling computing power

The virus lifecycle

- Infection – it reaches out to compromise then exploit a particular host
- Entrenchment – it digs in on the host, making removal difficult, and restricting access to tools to solve the problem
- Propagation – it seeks out new hosts and prepares to infect them

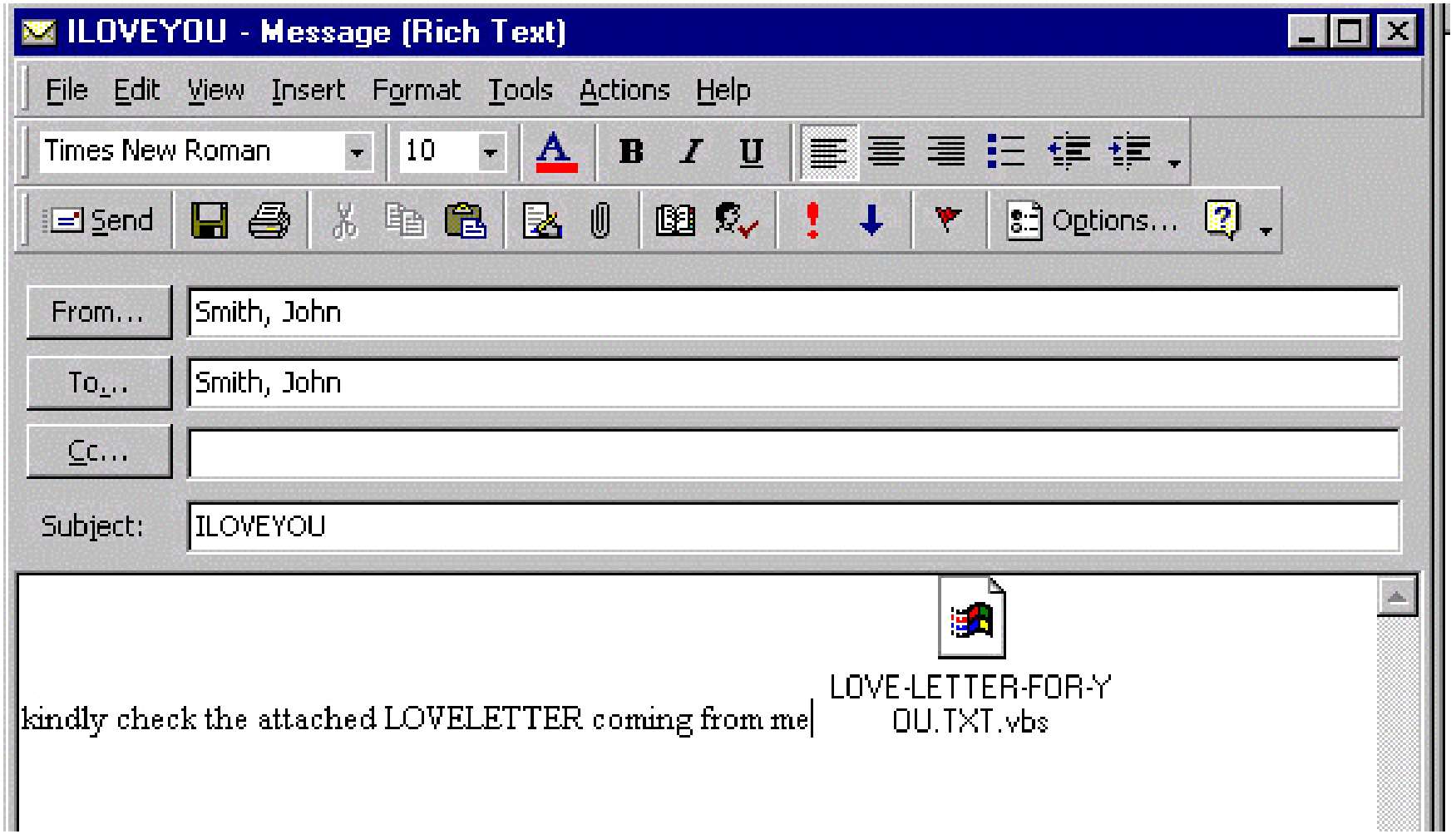
Payloads

- Post-infection – once you've compromised a host you can do it there and then. Deleting files, stealing confidential data
- Entrenchment – the host must remain operational. Sending spam, monitoring browsing, redirecting clicks for advertising revenue
- Propagation – the virus' goals are achieved in the act of spreading. Chain letters, pyramid schemes

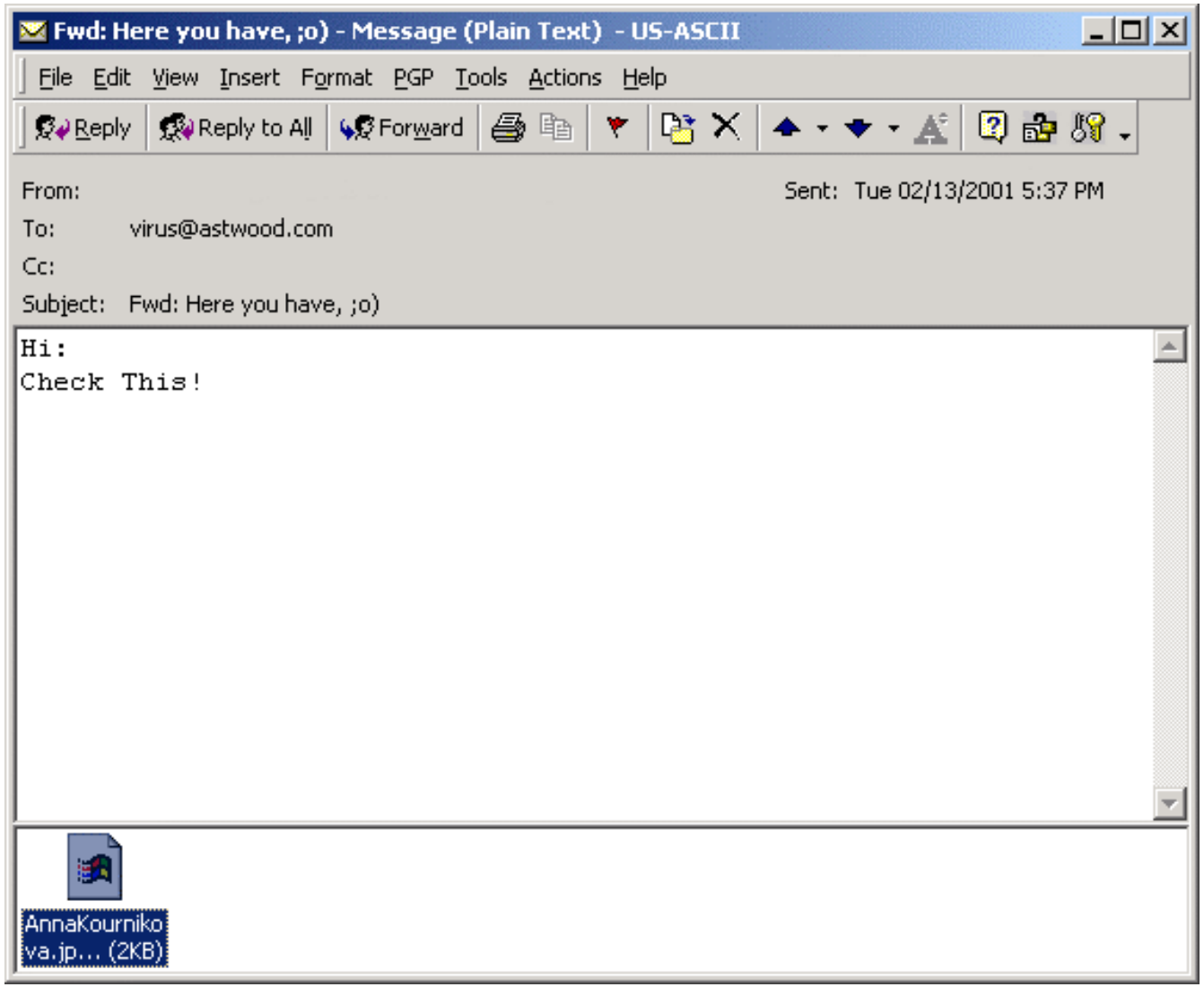
Propagation strategies

- Choice of medium
  - Email, IM, Web, Network-Level
- Choice of mechanism
  - Involuntary
  - Naivety
  - Deception
  - “The Pact”

Naivety


ILOVEYOU - Message (Rich Text)
File Edit View Insert Format Tools Actions Help
Times New Roman
10
Send
Options...
From...
Smith, John
To...
Smith, John
Cc...
Subject:
ILOVEYOU
kindly check the attached LOVELETTER coming from me
LOVE-LETTER-FOR-YOU.TXT.vbs

Deception


Fwd: Here you have, ;o) - Message (Plain Text) - US-ASCII
File Edit View Insert Format PGP Tools Actions Help
Reply Reply to All Forward
From:
Sent: Tue 02/13/2001 5:37 PM
To: virus@astwood.com
Cc:
Subject: Fwd: Here you have, ;o)
Hi:
Check This!
AnnaKourniko
va.jp... (2KB)

State of the art

- The best tricks of (deployed) viruses
  - restrict access to anti-virus sites
  - entrench and resist uninstallation
  - scan for vulnerable hosts intelligently
  - use multiple propagation strategies and mediums
  - control rate of propagation to avoid early detection
  - contain payloads which do not cripple the host

- So what's coming next to our inboxes?

Interactive propagation

- What if future viruses exploit *user interaction* – gain assistance with propagation, and negotiate entrenchment
- incoming … *"Hello Bob, this is Alice's virus. If you install me, you can view all Alice's files and email."*
- outgoing... *"Hello Alice, this is your virus speaking. If you don't design a message to spread me to Bob, I'll start deleting your files."*

Entrenchment

- Viruses need to survive to execute more powerful payloads, especially sending spam
- Interactive entrenchment techniques contact the user, and manipulate them in order to gain assistance (disabling A/V software) or simply to cause inaction
- *"Hello Alice, I'm the first ever reasonable virus. I'm not going to snoop your passwords, all I want to do is send a bit of spam. Try to uninstall me now and I'll dig in, I'll ruin your PC, you'll have to reinstall windows. But wait a week and I'll leave of my own accord, I promise!"*

Cross-platform entities

- Interactive virus instances must work together achieve their goals, otherwise you just turn off your PC, and the chatter stops.
- The virus now isn't a particular file on your PC, it isn't particular to your PC, it's a cross-platform network entity.
- Botnets and Zombies already use P2P communications and IRC/Email to talk to their creators and to each other.
- If your virus makes a threat, its friend can enforce it

The botnet entity

- Is a network of compromised hosts, communicating P2P, or by tuning in to a centralised but public service e.g. IRC, a particular web site.
- Has multiple layers. Often a stealth *deployment layer* downloads and installs a more overt payload layer. If the payload is detected and removed, the deployment layer remains untouched.
- Can monitor and reconfigure itself. Actually everything seen so far these days has been under direct human control, not AI
- A different bunch of humans build botnets to those who use them to send the spam. They are service providers in the spam economy.

More threats and rewards

Reward	Examples
Threat Enactment*	"I'll carry out threat X on Y, and you can watch!"
Privacy Invasion*	"You can browse X's hard drive"
	"You can read X's email archive"
	"You can watch X's webcam/mic"
Revelation*	"I'll tell you what X said to Y"
	"I'll tell you what I found on X's hard drive"
Fabrication*	"You can forge emails from X"
Mischief*	"You can seize control of X's PC"
Virtual goods	"You'll get tons of free porn"
	"You'll get free software"
Real-world goods*	"You'll get free goods to your door"
Innovation	"You can use this really cool feature"
Unsubstantiated	"You'll get seven years good luck"
	"Your true love will return to you"

Fig. 2. Taxonomy of Rewards (* marks cross-party rewards)

More threats and rewards (2)

Threat	Examples
Data Destruction	"I'll delete all your files"
Privacy Invasion*	"I'll forward emails from your archive daily to X"
Revelation*	"I'll tell X that you said Y to Z"
	"I'll tell X about the porn I found in your web cache"
	"I'll put all your data on the net, searchable from Google"
Fabrication	"I'll make up an email telling X you slept with Y"
Desecration	"I'll distort all your digital camera photos and reduce them to 1/4 size"
Framing	"I'll plant illegal images on your computer"
Hardware Damage	"I'll blow-up your monitor"
	"I'll re-flash your BIOS and kill your PC"
Security Exposure	"I'll sabotage your security" (Kleptographic attacks [12])
	"I'll harvest all your keystrokes and passwords"
	"I'll get your credit card number and abuse it"
Real-world*	"I'll order something using your credit card for my friend"
Unsubstantiated	"I'll get your sister beaten up"
	"I'll give you seven years of bad luck"
Nuisance	"I'll phone your mobile at all times of day and night"
Unwanted goods*	"I'll send unwanted goods to your door"
Reporting	"I'll report your illegal downloads to the RIAA"
Access Denial	"I'll prevent you from using Word or Excel"
Composite	"I'll bug you with a threat or reward every 15 mins"
	"Now we're going to play truth or dare"

Fig. 3. Taxonomy of Threats (* marks cross-party threats)

Ransom!

- *“Hello Bob, you’re a friend of Alice, aren’t you? I’m Alice’s virus, and I know a big dark secret of what I found on her hard drive. If you don’t install me within the next 48 hours, I’m going to tell the whole world Alice’s secret… you wouldn’t want that!”*

- Did you read the slide? Too late! You’ve already caught the virus…

The propagation continuum

- We have briefly surveyed propagation strategies which are clearly unethical and normally illegal
- Other software propagates too, often interactively through the user, and *allegedly* voluntarily
- AdWare spreads through web sites
- Commercial software spreads through file formats. I send you a PDF, you download Acrobat reader, read it. You send the PDF on, target downloads acrobat reader, acrobat reader spreads. Unethical? No. Propagation? Yes.
- What when the main purpose of the software is ethical, but it brings bundles of undesirable features?

Fighting interactive viruses

- Virus checkers can warn you when it's time to download the .EXE, but you may already be in the trap, held at ransom or blackmailed…
- Spam filters could intercept messages before you even read them, preventing the attack from reaching you.
- Educate the user to be wary of the promises of computer programs. Check what it will do before you click install! But who reads the entire licence agreement?
- It comes down to a battle to gain the physical attention of the user… interesting… the same battle fought every day in many types of media and advertising.

More information

- Richard Clayton

http://www.cl.cam.ac.uk/users/rnc1/

- Mike Bond

http://www.cl.cam.ac.uk/users/mkb23/